

NS 50 not assigned

CRIMINAL COURT OF THE STATE OF NEW YORK
NEW YORK COUNTY: PART D

-----X
THE PEOPLE OF THE STATE OF NEW YORK,

-against-

HELEEN MEES,

Defendant.
-----X

NOTICE OF MOTION

NO. 2013NY050589

Honorable Steve Statsinger

Oral argument requested ☒

PLEASE TAKE NOTICE that upon the annexed affidavit, duly sworn on the 8th day of March, 2018, upon the indictment and upon all those proceedings previously had herein, Defendant **Heleen Mees** will move this Court at the Courthouse, 100 Centre Street, New York, New York, before the Honorable Steven Statsinger, at a date and time to be fixed by the Court, for a petition for writ of coram nobis.

PLEASE TAKE FURTHER NOTICE, that Defendant reserves the right to make such further motions pursuant to C.P.L. § 255.20 (2) & (3) as may be necessitated by the Court's decision on the within motion and by further developments which, even by due diligence, Defendant could not now be aware.

18 MAR -8 PM 2:15

CRIMINAL COURT
CITY OF NEW YORK

Dated: March 8, 2018

Signature

A handwritten signature in black ink, consisting of a large, stylized 'M' with a long, sweeping vertical stroke on the left side.

HELEEN MEES
THE SWEENEY BUILDING
30 Main Street, Apt. 11H
Brooklyn, New York 11201
(917) 325-5877

Defendant Pro Se

To: Clerk of the Court
Hon. Steven Statsinger
District Attorney's Office

AFFIDAVIT OF SERVICE

State of New York)
County of Manhattan)

The undersigned being duly sworn, deposes and says:

H. Nijkamp is not a party to the action, is over
(name of person serving papers)

18 years of age and resides at 1 Main Street, Brooklyn, NY 11201

(complete address of person serving papers)

That on March 8, 2018, deponent served the within
(date of service)

Petition for writ of coram nobis

(name of document[s] served)

upon Manhattan District Attorney's office located at
(name of person/corporation served)

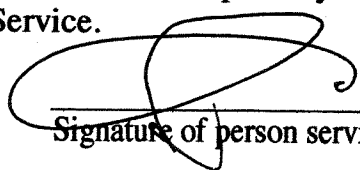
One Hogan Place, New York, NY 10013

(complete address where other party/corporation served)

(Select method of service)

☒ Personal Service: by delivering a true copy of the aforesaid documents personally;
deponent knew said person/corporation so served to be the person/corporation described.

☐ Service by Mail: by depositing a true copy of the aforesaid documents in a postpaid
properly addressed envelope in a post office or official depository under the exclusive care
and custody of the United States Postal Service.


Signature of person serving papers

H. Nijkamp
Printed Name

Sworn to before me this 8th
day of March, 2018


Notary Public

HUSEYIN SYUCEL
Notary Public - State of New York
NO. 01YU6288145
Qualified in New York County
My Commission Expires Aug 26, 2021

CRIMINAL COURT OF THE STATE OF NEW YORK
NEW YORK COUNTY: PART D

-----X
THE PEOPLE OF THE STATE OF NEW YORK,

**AFFIDAVIT IN SUPPORT
OF PETITION FOR WRIT
OF CORAM NOBIS**

-against-

NO. 2013NY050589

HELEEN MEES,

Defendant.

-----X

PETITION FOR WRIT OF CORAM NOBIS

RELIEF VACATE ADJOURNMENT IN CONTEMPLATION OF DISMISSAL

HELEEN MEES, defendant *pro se*, declares the following to be true under the penalty of perjury:

1. I am the defendant in this case. On February 22, 2018, Your Honor denied my motion to direct the District Attorney's Office to reopen the instant case against me as justice requires unsealing pursuant to C.P.L. § 160.50(1)(d)(ii). See Exhibit A. Your Honor argued that (1) the District Attorney has broad discretion in determining who shall be charged in a criminal case, and (2) prosecutors are not law enforcement agents under C.P.L. § 160.50(1)(d)(ii). See Exhibit B.

2. I understand that the District Attorney has broad discretion in determining who shall be charged in a criminal case and I do not wish to challenge that. However, a bedrock principle of U.S. and New York law is that the prosecutor must disclose evidence or information that would prove the innocence of the defendant. *See Brady v. State of Maryland*, 373 U.S. 83 S.

Ct. 1194; 10 L. Ed. 2d 215; 1963. The suppression of exculpatory evidence is a violation of a defendant's constitutional rights. The Supreme Court has held that Brady disclosures must also be made at the pre-plea stage (*United States v. Ruiz*, 536 U.S. 622 (2002)).

3. The First Department has ruled that a guilty plea can be overturned because of pre-plea Brady violations. In addition to the threshold *Brady* analysis, i.e., whether the evidence is material to the issue of guilt or punishment, the Appellate Division, First Department, has adopted a standard that also requires an analysis of whether the information, if disclosed, would have materially affected the defendant's decision to plead guilty (*People v Martin*, 240 AD2d 5, denied upon reconsideration, 92 NY2d 856). The Third Department has also followed this reasoning (*People v Drossos*, 291 AD2d 723).

4. I would never have accepted the Adjournment in Contemplation of Dismissal as an outcome had I known of the 1,251 unlawful surveillance images in the criminal file. In other words, I would not have accepted the ACD if I had known that I was the victim of a felony sex crime (Unlawful Surveillance in the Second Degree; Penal Law 250.45; 1,251 counts) and that the perpetrator, Willem H. Buiter, used the spoils of his crime to have me arrested. The 1,251 unlawful surveillance images go directly to my innocence. Not only did Buiter falsely accuse me of sending him the 1,251 naked photos, which purportedly "severely annoyed and alarmed" him, the 1,251 photos also serve as evidence that the romantic relationship continued three years beyond the professed end date of November 7, 2009.

5. In the related civil litigation, Buiter admits that the criminal file also includes a 1000 and potentially 2000 duplicates of emails that I purportedly sent him. This means that at least half and potentially three-quarter of the evidence in the criminal file is false. See Exhibit C, ¶14.

Moreover, Buiter misled the police and prosecution about the number of emails that he received in his home in Manhattan to make the police and the District Attorney's office believe they had jurisdiction. In reality, Buiter only moved from London to New York in March 2013, i.e., three months before my arrest. The number of emails Buiter received in his home in Manhattan is only a fraction of the emails complained of in the criminal complaint and the Information. The criminal prosecution for acts that I allegedly committed prior to March 1, 2013, i.e., the alleged sending of (unwanted) emails and the alleged (unwanted) meetings in Amsterdam and Beijing, violates not only federal due process but also international law.

6. The purpose of an ACD is "to provide a shield against the criminal stigma" that would otherwise attach to a defendant. *Lancaster v. Kindor*, 471 N.Y.S.2d 573, 579 (1st Dep't 1984); accord *Smith v. Bank of America Corp.*, 865 F. Supp. 2d 298, 302 (E.D.N.Y. 2012) (Weinstein, J.) (ACD designed to avoid persons charged with minor offenses being permanently designated as criminals). When granted an ACD, a defendant "is 'entitled to the full benefit of the record sealing and expunging provisions' that attend an acquittal." *Rothstein v. Carriere*, 373 F.3d 275, 287 (2d Cir. 2004) (quoting *Hollender v. Trump Village Co-op, Inc.*, 58 N.Y.2d 420 (1983)). The arrest and prosecution become a nullity (CPL § 170.55(8)), the record of the action is sealed (CPL § 160.50(3)(b)), and the defendant shall be restored "to the status he occupied before his arrest and prosecution." CPL § 170.55(8). The ACD statute specifically provides that "[n]o person shall suffer any disability as a result" of an ACD. *Id.* "The over-all effect of a consummated ACD dismissal is then to treat the charge as though it never had been brought." *Hollender*, 58 N.Y.2d at 425 (emphasis added).

6

7. I am deprived of all the above benefits. I lost my NYU professorship, my job as a newspaper columnist, and all my lobbying and consulting business. While the courts recognize that the “ability to earn a living is an important factor in avoiding criminality” through an ACD, *Smith*, 865 F. Supp. 2d at 300, the false accusation that I “sent Buiter naked pictures of myself masturbating”, the public airing of my private conversation, and the public ridicule that followed my arrest and prosecution, make it virtually impossible for me to earn a living, more than four years after the ACD was entered. I clearly suffer, and will continue to suffer, a “disability as a result” of my prosecution.

8. When I found out about the 1,251 unlawful surveillance images on October 13, 2014, my attorneys asked ADA Schott for an investigation by letter of October 20, 2014. See Exhibit D. When we did not hear from ADA Schott, my attorneys on October 27, 2014, sent a letter to District Attorney Vance asking for an investigation and a dismissal of the charges. See Exhibit E. We were told by ADA Nitin Savur to come back if we had more evidence.¹ As soon as we had the forensic report, we again asked District Attorney Vance by letter of May 9, 2016, for an investigation and the dismissal of the charges. See Exhibit F. I was rebuffed each time.

9. Because the news of my arrest and prosecution was reported around the globe and every detail of Buiter’s lurid accusations against me is preserved on hundreds of websites, the ACD is not sufficient to return me to a state as though the prosecution “never had been brought.” The “full benefit” of sealing and expunging the record did not make my arrest and prosecution a “nullity.” Nor is the ACD in any way sufficient to restore my previous status. These consequences may be understandable, and could even be justifiable, were it not for the fact that the District

¹ According to ADA Savur, the ACD could also be undone once the case was sealed.

Attorney's office prosecuted the victim of a felony sex crime, that is, me, at the instigation of the perpetrator, Buiter. Therefore, I petition for a writ of coram nobis relief to undo the Adjournment in Contemplation of Dismissal; I must either be acquitted at trial or the charges against me must be dismissed in the interest of justice.

10. Historically, the ancient writ of "error coram nobis" was used by courts to correct errors for which no other avenue of judicial relief was apparent (see e.g. *People v Hairston*, 10 NY2d 92, 93-94 [1961]; *People v Bachert*, 69 NY2d 593, 598-600 [1987]). The enactment of the Criminal Procedure Law "did not expressly abolish the common-law writ of coram nobis or necessarily embrace all of its prior or unanticipated functions" (*People v Bachert*, 69 NY2d at 599). The Court of Appeals authorized a limited exception to the one-year rule if diligent and good-faith efforts to comply with the requirement were deliberately thwarted by the People (see *People v Johnson*, 69 NY2d 339, 341-342 [1987]; *People v Thomas*, 47 NY2d at 43).

11. The ancient writ "continues to be available to alleviate a constitutional wrong when a defendant has no other procedural recourse" (*People v Syville*, 15 NY3d 391). My counsel, Ira D. London, was ineffective because he did not move this Court in 2014 to undo the ACD even though I asked him to. While the instant case, strictly speaking, does not concern appellate rights, it obviously does concern constitutional wrongs where the defendant has no other procedural recourse and was deliberately thwarted by the People (*People v. Andrews* (Court of Appeals, 2014)). The constitutional wrongs are suppression of exculpatory evidence and ineffective counsel and the lack of procedural recourse is clear from Your Honor's Decision and Order of February 22, 2018.

CONCLUSION

WHEREFORE, for the foregoing reasons, I respectfully petition for a writ of coram nobis relief to vacate the Adjournment in Contemplation of Dismissal, and that this Court issue any other relief it deems just and equitable.

Signature



HELEN MEES
THE SWEENEY BUILDING
30 Main Street, Apt. 11H
Brooklyn, New York 11201
(917) 325-5877

Defendant Pro Se

Sworn to before me this 8th day of March, 2018



CATHERINE ERCOLE
Notary Public - State of New York
No. 01ER6214008
Qualified in New York County
Commission Expires November 23, 2021

To: Clerk of the Court
Hon. Steven Statsinger
District Attorney's Office

CRIMINAL COURT OF THE STATE OF NEW YORK
NEW YORK COUNTY: PART D

-----X
THE PEOPLE OF THE STATE OF NEW YORK,

NOTICE OF MOTION
2013NY050589

-against-

HELEEN MEES,

Defendant.


-----X
PLEASE TAKE NOTICE that upon the annexed affirmation of **Joshua D. Kirshner, Esq.**, duly affirmed on the 24th day of January, 2018, upon the indictment and upon all those proceedings previously had herein, Defendant **Heleen Mees**, by undersigned counsel, will move this Court at the Courthouse, 100 Centre Street, New York, New York, before the Honorable Steven Statsinger, at a date and time to be fixed by the Court, to to direct the District Attorney's Office to unseal and reopen the instant case against Heleen Mees as justice requires unsealing pursuant to C.P.L. § 160.50(1)(d)(ii).

PLEASE TAKE FURTHER NOTICE, that Defendant reserves the right to make such further motions pursuant to C.P.L. § 255.20 (2) & (3) as may be necessitated by the Court's decision on the within motion and by further developments which, even by due diligence, Defendant could not now be aware.

Dated: New York, New York
January 24, 2018

Respectfully submitted,

BRAFMAN & ASSOCIATES, P.C.
767 Third Avenue, 26th Floor
New York, New York 10017
(212) 750-7800


By: Joshua D. Kirshner

To: Clerk of the Court
Hon. Steven Statsinger
District Attorney's Office

CRIMINAL COURT OF THE STATE OF NEW YORK
NEW YORK COUNTY: PART D

-----X
THE PEOPLE OF THE STATE OF NEW YORK,

-against-

ATTORNEY'S
AFFIRMATION
2013NY050589

HELEEN MEES,

Defendant.

-----X
STATE OF NEW YORK)
COUNTY OF NEW YORK) ss:

JOSHUA D. KIRSHNER, being an attorney at law duly admitted to practice in the courts of New York, affirms the following to be true under the penalty of perjury:

1. I am an attorney in the law firm of **BRAFMAN & ASSOCIATES, P.C.**, attorneys for defendant Heleen Mees, and I make this affirmation in support of a motion dated January 24, 2018, whereby Defendant moves for this Court to direct the District Attorney's Office to reopen the instant case against Heleen Mees as justice requires unsealing pursuant to C.P.L. § 160.50(1)(d)(ii).

2. **This affirmation is made upon information and belief.** The sources of information and the grounds for such beliefs are materials previously disclosed by the District Attorney's Office, conversations with numerous individuals, applicable legal authorities, and those other records and materials constituting counsel's file.

MOTION TO UNSEAL

3. On July 1, 2013, Dr. Heleen Mees (“Mees”), a New York University economics professor, political commentator, author, and public figure in her country of origin, the Netherlands, was arrested in New York City on various charges which stem from a complaint by a fellow economics professor and chief economist of Citigroup, Willem H. Buiter (“Buiter”). Buiter incited the police to arrest Mees by making a series of false statements to the police and the Manhattan District Attorney’s office, including that Mees harassed him by sending naked photos of herself.

4. As a result of Buiter’s allegations, Mees spent four days in jail at Rikers Island and the matter was highly publicized all over the world, including on the front page of the New York Daily News. See Exhibit A. Following her arrest, Mees lost her job as a professor at New York University, all her columns in international magazines and newspapers, as well as her speaking engagements and consulting jobs. Due to the publicity surrounding this matter, Mees has been unable to obtain gainful employment and is left with virtually no sources of income. Because of all that has transpired since her arrest and prosecution, Mees suffers from posttraumatic stress disorder and dysthymia (chronic depression).

5. In view of the substantial falsehoods in the criminal complaint, the Manhattan District Attorney’s office offered in March 2014 to discontinue the criminal prosecution of Mees by way of an Adjournment in Contemplation of Dismissal (ACD). Eager to avoid a public trial, primarily for financial reasons and to avoid further reputational and emotional harm, Mees consented to the ACD, which was entered by the Honorable Steven Statsinger on March 10, 2014.

6. Even though the Manhattan District Attorney's office acknowledged that there was no ground for her prosecution, Buiter continued his libelous campaign against Mees, repeating his false accusations of stalking and harassment in an elaborate public posting on Facebook of March 10, 2014. On June 26, 2014, Mees filed a complaint against Buiter in the New York Supreme Court, Kings County, on various grounds, including defamation, false arrest, and intentional infliction of emotional distress.

7. Buiter responded on October 6, 2014, with a motion to dismiss to which he attached 1,251 naked photos of Mees, claiming that she had sent him those photos. Dr. Mees saw the naked photos for the very first time on October 13, 2014, when her attorney forwarded her "Exhibit L", which was an email with 4 PDF-files attached thereto containing 1,251 naked photos. Buiter was, however, unable to produce any of the hundreds of emails to which the photos were purportedly attached. Contrary to what Buiter had represented to the police and prosecution, the 1,251 naked photos were surreptitiously and illegally taken by Buiter himself during his intimate Skype interactions via Skype webcam with Dr. Mees.

8. On October 20, 2014, Mees's attorneys, Ira D. London and Olav Haazen, sent a letter to Assistant District Attorney Samantha Schott to alert her to the fact that the Manhattan District Attorney's office had prosecuted the victim of a felony sex crime while protecting the man who is most likely the perpetrator. Schott did not respond to the letter. On October 28, 2014, London and Haazen sent a letter to Manhattan District Attorney Cyrus Vance, demanding an investigation into the 1,251 naked photos and an immediate dismissal of all the charges in the interest of justice. On November 18, 2014, Mees's attorneys met with Assistant District Attorney

Nitin Savur, who is a member of District Attorney Cyrus Vance's Executive Team. He told them that the District Attorney's office declined to investigate the matter.

9. Meanwhile Buiter refused to produce the 1,251 naked photos in JPEG-format of his own volition. Buiter successfully opposed discovery in the Federal Court, the Supreme Court, Kings County, and in the Amsterdam Civil Court. Only after a decision by the U.S. Court of Appeals, Second Circuit, of July 17, 2015, Buiter was ordered to hand over the 1,251 photo files in JPEG-format. After Buiter produced the JPEG files, Dutch counsel for Mees commissioned forensic experts SBV Forensics to examine all 1,251 photographs and all forensically imaged computers that Mees has had in her possession since 2008. Based on this forensic analysis, SBV Forensics concludes that it is a near certainty that Mees did not take the photographs, either with a phone, a standalone camera or a webcam, and that it is beyond a reasonable doubt that she did not send the photographs from any of her devices (the SBV Forensics report is attached as Exhibit B).

10. Specifically, SBV Forensics concludes with respect to the photo files:

- a. Because the photos were produced in both PDF (1,388) and JPEG format (1,251), it can be determined through a comparison of MD5 hash values and "data carving" that Buiter in fact had more unique naked photos of Mees in his possession than he represented (1,288 instead of 1,251). Among both the PDFs and the JPEGs there were also many duplicates (pp. 3-6).
- b. Based on Mees's position in the photos, it is impossible that she manually took the photos herself. Because variations between successive pictures

are mostly minor, which indicates only minimal intervals between them, it is also highly unlikely that the photos were taken in auto mode with a timer (pp. 6, 19-20).

- c. The format of the photos (640 pixels by 480 pixels, for a total of some 300,000 pixels) is inconsistent with the use of a digital camera. Images taken with digital cameras are measured in millions of pixel (“megapixels”) (pp. 7, 19).
- d. The pictures’ VGA resolution is, however, consistent with the use of either a webcam or a mobile phone camera (pp. 7-8, 19).
- e. The low number of EXIF metadata captured on the JPEG files is inconsistent, however, with the photos having been taken with a mobile phone. It is also inconsistent with the use of a digital camera. Both would have registered additional metadata, such as various characteristics of the camera lens or the brand and type of the phone used (pp. 8, 19).
- f. The EXIF metadata that was found, e.g. data indicating that no flash was used, excludes the possibility that the photos were stills derived from video footage (which does not register any information on the use of a flash) (pp. 8, 19).
- g. The depth and camera angles of the photos are also consistent with the use of a webcam (pp. 7, 19).
- h. The picture files are consistent with still images taken during a live video chat on a platform like Skype. If the screenshots were taken on an Apple

computer, however, such as used by Mees, Apple's operating system (Mac OS X) would have saved them as PNG files—not, as is the case here, as JPEGs (pp. 8-9, 19).

- i. Photo Booth, which is a standard Apple application does save photos in JPEG format but the photos' metadata is inconsistent with the use of Photo Booth because such use would have automatically registered the application's name as an IPTC field in each file (p. 9).
- j. The photos have a resolution of 96 dpi, which is also not consistent with the use of Apple computers or digital cameras, which automatically generate images with resolution of 72 dpi. The photos' 96 dpi resolution is, however, consistent with the use of a Windows computer (which Mees believes Buiter uses exclusively) (p. 10).
- k. There is no indication on any of Mees's Apple computers that any metadata or file characteristics were manually manipulated. Manual editing would require opening, editing and re-saving each of the 1,288 unique picture files individually and would therefore be extremely time-consuming. No Windows programs and no virtualization software were found on any of Mees's laptops (pp. 10, 19).

11. With respect to Buiter's possession of the photos but not the emails by which they were supposedly transmitted, SVB Forensics concludes:

- a. It is virtually certain that the photos were never on Mees's laptops. If they were, it would have been possible to retrieve or restore the files

forensically. It is nearly impossible and technically very complex to individually remove files in a manner that guarantees the user that the files are forever irretrievable (pp. 11-15, 19-20).

- b. Secure removal of email files in a way that makes retrieval impossible also requires highly specialized knowledge of the workings of the Mac OS X operating system. No emails of the kind Buiter claims existed were found, however, on Mees's computers (pp. 13-15, 20).
- c. The "rule" that Buiter claims explains why the photos were saved, while the emails purportedly attaching them were deleted, would in principle have saved identical pictures only once, overwriting prior versions of the same attachment or make. The presence of duplicates of photos in Buiter's files is inconsistent with such workings of the rule (pp. 17-18).
- d. The rule is also inconsistent with the fact that a different picture ("moi.jpg"), which the parties agree Mees did send Buiter (more than once) and for which Buiter can produce the emails to which it was attached, was not saved in the same attachment folder, and that yet a third picture Mees sent ("plaatje.jpg") was also not saved there (p. 18).
- e. Taking into consideration that the file names contain only a sequential number as well as the fact that numbering did not restart at the first picture from a new session, it is a near certainty that Buiter changed the file names before handing them to the police and the Manhattan District Attorney's office.

12. Accordingly, Buiter's excuse for his possession of photos of Mees's private parts is not supported by forensics. This leaves no other reasonable explanation than that Buiter took the photos. The forensic investigation also corroborates Mees's account that their intimate interactions via Skype were never meant to be recorded, that she was unaware of the recordings, and that she never consented to being recorded.

13. Buiter alleged in the Dutch proceedings that he 'accidentally' saved the 1,251 naked photos on the hard-drive of his computer in London. Buiter also alleged that he threw that computer away in December 2012 while still in London and that he destroyed the external hard-drive on which the naked photos were saved in December 2013. This course of action, however, is not compatible with the finding of the 1,251 naked photos in Buiter's American cloud service, of which Buiter's Dutch counsel, Jeroen Kortmann, informed the Amsterdam Civil Court in a letter of November 17, 2015.

14. The only explanation for the 1,251 naked photos ending up in Buiter's American cloud service is that he saved the photos on his mobile devices, which cannot happen accidentally. The 1,251 naked photos were thus also not accidentally saved on Buiter's computer in London. Since Buiter did not move to the United States and thus did not start using his American cloud service until April 2013, the finding of the naked photos in his cloud service shows that Buiter held on to the pictures on his personal devices until well into 2013, while he was reporting Mees to the police (Buiter's provider only automatically backs up mobile devices). That means that Buiter was on the one hand complaining to the police about Mees's advances and nudity, while on the other hand enjoying her nudity on his handheld devices.

15. Buiter has so far refused to hand over the 1,251 photo files in PNG-format that were found in his cloud service even though his Dutch counsel promised the Amsterdam Civil Court in a letter of November 17, 2015, that the PNG-files would be handed over to Mees's attorneys. The PNG-files, presumably, contain information as to when and by whom the 1,251 naked photos were made. If it is clear when the photos were made, the information can easily be compared with the Skype chats Buiter and Mees had. In case the timing of the photo files matches the Skype chats, it is 100 percent certain that Buiter recorded Mees. After all, the 1,251 naked photos were taken on a Windows computer while Mees used a white MacBook computer, on which the Skype chats were locally stored.

16. In an affidavit of August 11, 2015, filed in the Supreme Court, Kings County, Buiter categorically denies that he and Mees "ever had a Skype session in which either of us disrobed in any way or engaged in any kind of sexual act". See Exhibit C. This statement can easily be proven to be false with a 300-page record of Skype sessions between Buiter and Mees from November 2010 through July 2012. Why would Buiter make false statements under oath about the fact that he and Mees frequently engaged in intimate acts via Skype webcam if not to obscure the fact that he surreptitiously recorded Mees?

17. The only reason Buiter's computer and external hard drive on which the 1,251 photo files were originally saved are no longer available for forensic examination to determine if it was used to take the naked photos of Mees, is because Buiter threw them away by December 2013. In other words, Buiter destroyed key evidence pending the Manhattan District Attorney's criminal prosecution of Mees, in which the alleged sending of naked photos was a significant issue for trial. Mees should not be prejudiced because Buiter willingly and knowingly destroyed

his computer and external hard drive in a clear act of spoliation. Therefore, an adverse inference against Buiter with respect to the 1,251 naked photos is more than justified.

18. The unlawful surveillance of private parts is a felony sex crime pursuant to New York Penal Law § 250.45 and can make the offender not only liable for jail time, but also for registration on the sex offender registry. Under settled case law, Mees has a reasonable expectation of privacy during consensual sexual encounters. “When a person knowingly undresses and engages in sexual relations with another person, he or she should be able to do so with the reasonable expectation that his or her actions are limited to that particular time and place and that his or her naked body and/or sexual acts will not be memorialized and/or repeatedly viewed at any time by the other person present or by anyone else with whom that person decides to share the recordings (*see Wallace v. State*, 961 NE2d 529, 533 [Ind Ct App 2012]; *Lewis v. LeGrow*, 258 Mich App 175, 188-189, 670 NW2d 675, 684-685 [Mich Ct App 2003]).” *New York v. Piznarski*, N.Y. Slip Op. 08157 (3rd Dept., 2013).

19. It has been extraordinarily distressing for Mees to know that Buiter recorded their intimate love play via Skype webcam and held onto the naked photos on his mobile devices while he was reporting her in July 2013 to the New York Police Department and the Manhattan District Attorney’s office. Buiter’s actions have caused Mees anxiety, nightmares, nausea and vomiting, abnormal weight loss, emotional numbness, difficulty concentrating, and loss of interest in life. Buiter’s actions have also caused her intense feelings of shame, mistrust, and betrayal.

20. Buiter not only used the 1,251 naked photos to incite Mees’s arrest and prosecution, he and his lawyers also threatened Mees with publication unless she would

discontinue all legal proceedings against Buiter here and abroad and sign a Non-Disclosure Agreement. These threats of publication continued even after the Supreme Court, Kings County, on November 20, 2014, ordered the civil case to be treated as a matrimonial case. The Amsterdam Civil Court deemed the threat of publication by Buiter and his lawyers, Tim Keane, Adrienne Koch, and Jeroen Kortmann, so credible that on November 19, 2015, the Court issued a gag order prohibiting Buiter, his wife, and his lawyers to publicize the 1,251 naked photos or their existence.

21. On January 26, 2015, Mees's attorneys filed a request under the Freedom of Information Law (FOIL) with the Manhattan District Attorney's office for a copy of all official records and documents in her case file. On November 17, 2015, Mees received the FOIL production, including about 1200 naked photos of her (the photos are available for in camera review). The naked photos were never disclosed during plea discussions even though a layman can see that these are screenshots and not "selfies" (Mees's hands are visibly otherwise occupied in each single frame).

22. It's not like the District Attorney's office could not have known that Buiter and Mees frequently engaged in sexual acts via webcam. On the contrary, the Omnibus Motion that Mees filed in this Court on October 10, 2014, specifically states that Buiter and Mees, in addition to their monthly romantic encounter dates, 'spent dozens of hours each year on Skype' and that 'Buiter would regularly masturbate in front of the camera, using the online video-service.' See Omnibus Motion, ¶9; and Reply Affirmation in Support of Omnibus Motion, ¶16h. The Omnibus Motion also states that Mees sent Buiter only one selfie and that 'she did not send him any other selfies even though Buiter repeatedly asked her to'. See Omnibus Motion ¶2.

23. The naked photos constitute exculpatory evidence that the District Attorney's office should have disclosed during plea discussions (*Brady v. State of Maryland*, 373 U.S. 83 S. Ct. 1194; 10 L. Ed. 2d 215; 1963). Even after the Manhattan District Attorney's office had been put on notice by letter of October 20, 2014, that any naked photos of Mees in the criminal file were the product of unlawful surveillance and, therefore, exculpatory, the Manhattan District Attorney's office refused to share the photo files with Mees. The District Attorney's office made Mees file a FOIL request instead to which the District Attorney's office only responded 11 months later. The Freedom of Information Law §89(3)(a) states that a government entity has only five business days to respond to a FOIL request (which may be extended to 20 business days). The Manhattan District Attorney's office thus actively obstructed Mees's quest for justice.

24. The report by SBV Forensics shows that Buiter made false representations to the police and the Manhattan District Attorney's office when he told them that Mees had sent him naked photos of herself and that her actions severely annoyed and alarmed Buiter. In the Information of August 5, 2013, Buiter claimed he had broken off all relations with Mees on November 7, 2009, and that she had harassed him ever since. As Buiter secretly made screenshots of Mees's private parts in 2011 and 2012, it is safe to conclude that the romantic relationship between Buiter and Mees lasted at least three years longer than Buiter had represented to the prosecution. The 1,251 naked photos are also impeachment evidence, that is, they go to the credibility of Buiter as a witness. The 1,251 naked photos show that Buiter has no qualms about lying under oath to the police, the prosecution, and the courts, that he has no qualms about tampering with and fabricating evidence, and that he also has no qualms about extorting Mees into giving up all her legal claims against him.

25. The Manhattan District Attorneys' office showed gross negligence when it accepted the 1,251 nude photos from Buiter as evidence of stalking and harassment without any further questions asked. For a Special Victims Bureau that prides itself on being the best in the country, it is shockingly amateurish. Buiter has stated in the related civil litigation in the Netherlands that he handed Assistant District Attorney Samantha Schott hard copies of the photos and a USB-stick containing one pdf-file with all photo files combined. Why would a victim of stalking – instead of simply handing over the original photo files – go to such great lengths to manually combine 1,251 purportedly alarming photos in one pdf-file if not to disguise the metadata of the individual photo files? That fact alone should have set off alarm bells.

26. Even though Buiter was unable to produce any of the 'hundreds of emails' to which the 1,251 photos were purportedly attached, the Manhattan District Attorney's office did not even ask Buiter for the original photo files. At the time, Buiter's external hard drive was still available for forensic examination. The fact that Assistant District Attorneys Samantha Schott and Jeanine Launay never mentioned the 1200 naked photos during the plea discussions with Mees's attorneys, suggests that they were well aware that the photos were exculpatory but chose not to investigate and not to alert Mees or her lawyers to their existence. Schott and Launay must have realized that Mees would never have accepted the ACD as an outcome had she known that the criminal file included 1200 unlawful surveillance images of her.

27. In a letter of May 8, 2016, to District Attorney Cyrus Vance, Mees's attorneys reiterated their request for an investigation into Buiter's possession of the 1,251 naked photos based on the Forensic Report. On July 5, 2016, they met with Assistant District Attorneys Audrey Moore, chief of the Special Victims Bureau, and Vanessa Puzio. Moore, who is also a

member of District Attorney Cyrus Vance's Executive Team, told Mees's attorneys that the District Attorney's office is not able to prosecute Buiter because he destroyed the computer and external hard drive on which the images had originally been saved. It would, therefore, be impossible to prove beyond a reasonable doubt that Buiter took the photos. At the same time, Moore declined to subpoena the 1,251 photo files in PNG-format that have been found in Buiter's cloud service and most likely contain information as to when and by whom the photos were taken, ostensibly because the report by SBV Forensics does not amount to probable cause. It reinforces the impression that District Attorney Cyrus Vance and his team are simply protecting a powerful Wall Street banker and the bank he works for, Citigroup.

28. Dr. Mees now moves this Court to undo the Adjournment in Contemplation of Dismissal; she must either be acquitted at trial or the charges against her must be dismissed in the interest of justice.

WHEREFORE, for all the above-stated reasons, and for those further reasons stated in the accompanying memorandum of law, the defendant's motion should be granted in all respects.

Dated: New York, New York
January 24, 2018

Respectfully Submitted,


Joshua D. Kirshner, Esq.

CRIMINAL COURT OF THE STATE OF NEW YORK
NEW YORK COUNTY: PART D

-----X
THE PEOPLE OF THE STATE OF NEW YORK,

-against-

MEMORANDUM OF LAW
2013NY050589

HELEEN MEES,

Defendant.

-----X

Statement of Relevant Facts

The facts of this case, insofar as pertinent to the within motion, are contained in the accompanying affirmation of Joshua D. Kirshner, Esq., duly affirmed on the 24th day of January, 2018 (“Affirmation”) and the exhibits appended thereto, all of which are incorporated herein and made a part hereof.

After a sealing order issues, C.P.L. 160.50(1)(d)(ii) authorizes a motion by any law enforcement agency, but authorizes unsealing only if justice requires release of the documents to the very agency making the motion. We see no reason the District Attorney should not be directed to do so under these circumstances as clearly justice requires it.

Additionally, while the granting of an ACD is not a conviction or an admission of guilt, it also is not a determination on the merits or an acquittal. CPL Section 170.55(8); *Matter of Marie B.*, 62 N.Y.2d 352, 477 N.Y.S.2d 87, 465 N.E.2d 807 (1984); *Malanga v. Sears, Roebuck and Co.*, 109 A.D.2d 1054, 487 N.Y.S.2d 194 (4th Dept.), *affd.*, 65 N.Y.2d 1009, 494 N.Y.S.2d 302, 484 N.E.2d 665 (1985). Thus, notwithstanding the statutory provision that “no person shall suffer any disability or forfeiture” as a result of the ACD (CPL Section 170.55[8]), a plaintiff,

for example, in a malicious prosecution action cannot establish that the criminal action was terminated in his favor, a necessary element of a cause of action for malicious prosecution. *Hollender v. Trump Village Cooperative, Inc.*, 58 N.Y.2d 420, 425–26, 461 N.Y.S.2d 765, 448 N.E.2d 432 (1983); *Lancaster v. Kindor*, 98 A.D.2d 300, 308, 471 N.Y.S.2d 573 (1st Dept.1984), *affd.*, 65 N.Y.2d 804, 493 N.Y.S.2d 127, 482 N.E.2d 923 (1985).

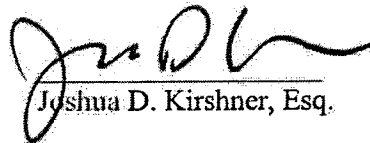
Thus, there is a procedural mechanism available and ample reason for the Court to intervene and ensure that justice is carried out in this case.

CONCLUSION

For the foregoing reasons, we respectfully request that this Court direct the District Attorney unseal this matter and reopen the case against Mees.

Dated: New York, New York
January 24, 2018

Respectfully Submitted,


Joshua D. Kirshner, Esq.

CRIMINAL COURT OF THE CITY OF NEW YORK
COUNTY OF NEW YORK: PART JURY 5

-----X
THE PEOPLE OF THE STATE OF NEW YORK

-against-

HELEEN MEES,

Docket No. 2013NY050589
Order

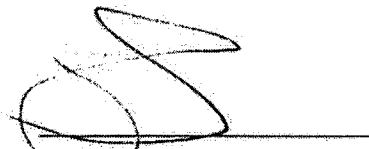
Defendant.

-----X
STEVEN M. STATSINGER, J.

By Notice of Motion, served on the District Attorney of New York County and filed with the Court on January 24, 2018, the defendant requests this court to direct the People to unseal this case and investigate what the defendant alleges was a malicious prosecution.

This request must be denied. First, the District Attorney has broad discretion in determining who shall be charged in a criminal case (*see United States v. Lovasco*, 431 US 783 [1977]; *People v. Harding*, 44 AD2d 800 [1st Dept 1974]; *People v. Muka*, 72 AD2d 649 [3d Dept 1979]; Pitler, New York Criminal Practice under the CPL, §5.27, p 267). Second, the Court of Appeals has stated that prosecutors are not law enforcement under Criminal Procedure Law § 160.50[1][d][ii] (*see Katherine B. V. Cataldo*, 5 NY3d 196 [2005]).

Dated: February 22, 2018
New York County, New York


Steven M. Statsinger
Judge of the Criminal Court

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF KINGS

-----X
HELEEN MEES,

Plaintiff,

-against-

WILLEM H. BUTER,

Defendant.
-----X

Index No. 9579/2014
(IAS Part 80,
Edwards, J.)
MOTION SEQUENCE #002

REPLY AFFIDAVIT OF
WILLEM H. BUTER IN
FURTHER SUPPORT OF
MOTION TO DISMISS

STATE OF NEW YORK)
 : ss.:
COUNTY OF NEW YORK)

WILLEM H. BUTER, being duly sworn, deposes and says:

1. I am the defendant in this action, and make this reply affidavit in further support of my motion to dismiss the complaint of plaintiff Heleen Mees ("Mees") and for other relief. Except where expressly indicated, the facts set forth herein are based on my personal knowledge.

2. As mentioned in my October 1, 2014 affidavit in support of my motion to dismiss ("Moving Affidavit"), I received from Mees thousands of emails, as well as numerous other communications. Emails I received from Mees during 2012 and 2013 were received almost entirely at one or another of two personal email accounts I maintained, initially one through BTInternet, and thereafter one through Gmail. For a time I had emails received at my BTInternet account automatically forwarded to my Gmail account. During this period I accessed email using one or another of three computers, each of which used Microsoft Outlook for handling email, and one or another of two phones.

3. Prior to February 27, 2013 (when my attorney sent Mees a cease-and-desist letter) I made no effort to retain all of the numerous and very repetitive e-mails I received from Mees.

I had often placed Mees's emails in an Outlook folder called "Garbage". Such a folder existed on each of my computers. Since Mees's email messages were repetitive beyond belief, many I simply deleted.

4. During March 2013, immediately after my attorney sent Mees a cease-and-desist letter, from my three computers I collected all emails I had previously received from Mees, to the extent that they were still available, and consolidated them. When I was consolidating all these emails from Mees a Microsoft Windows dialog box labeled "Replace or Skip Files" opened frequently. Each time this dialog box opened I clicked on the "Replace" option, which I understood deleted any duplicate email files I retrieved from my three computers. I believed that the Microsoft Windows program recognized all duplicate files, and that by selecting "Replace" I eliminated all duplicates.

5. Even consolidated into a single folder these thousands of email files were unwieldy to manage. These Microsoft Outlook files were cumbersome; to review each one each file had to be opened separately. Thus, at that time I started copying the thousands of individual Microsoft Outlook files into a small number of pdf files. These pdf files can contain thousands of pages of emails and allow one to read swiftly through a large number of emails without having to open each individual Microsoft Outlook (email) file.

6. After my attorney sent Mees a cease-and-desist letter I also started saving emails received from Mees as they were received. I became even more concerned about preserving evidence of Mees' incessant unsolicited communications on the evening of May 6, 2013, when Mees asked the doorman at our building to let her up to our apartment. I continued to collect Mees's messages until Mees was arrested on July 1, 2013, and from time to time copied these email messages into pdf files.

7. During May 2013 I provided the New York Police Department (“NYPD”) pdf copies of some emails I had received from Mees and on June 13, 2013 I forwarded to the NYPD additional emails Mees sent after the NYPD began its investigation. After July 1, 2013 but prior to August 5, 2013 I provided an Assistant District Attorney copies of additional emails I had received from Mees before July 1, 2013.

8. In support of my motion to dismiss, I submitted an affidavit sworn to on October 1, 2014 (“Moving Affidavit”). Exhibit “G” to that affidavit is a disc containing a single pdf file containing copies of each email Mees sent to me from July 12, 2012 through July 1, 2013 (with the limited exception of those emails that contain photographs of people, some nude). As mentioned above, it is substantially less cumbersome to review a single pdf document containing thousands of emails than it is to open thousands of individual Microsoft Outlook files. Exhibit “G” is a single pdf file containing 3,487 pages. Since most of Mees’s emails seemed to be single pages, it seemed very clear that the emails received from July 12, 2012 through July 1, 2013 totaled at least 3,000.

9. As discussed in the Moving Affidavit, Mees frequently sent me the same email repeatedly in such rapid-fire succession that I received multiple emails within seconds. Therefore, that Exhibit “G” included seemingly-identical emails containing the same message with the same date/hour/minute comported with the rapid fire with which Mees sent emails, so I did not understand them to be duplicates. However, I am now advised by Collin Bentley, a forensic computer expert retained by my counsel, that from July 12, 2012 through July 1, 2013 Mees sent me at least 2,509 emails and that Exhibit “G” does contain some duplicates.

10. At no time did I ever intentionally duplicate any of Mees’s emails, which were quite voluminous in any event. To my knowledge, any duplication must have been the result of

my collection of Mees's emails from two personal email accounts and three different computers, together with my belief, apparently in error, that clicking "Replace" each time Microsoft Windows "Replace or Skip Files" dialog box opened enabled me to avoid saving duplicate Microsoft Outlook (email) files.

11. Though in opposition to my motion to dismiss Mees submitted no affidavit denying that she sent me thousands of emails between July 12, 2012 and July 1, 2013 or denying that she frequently sent me emails in such rapid-fire succession that multiple copies arrived within the same minute, and I am advised by Mr. Bentley that his analysis confirms that I received from Mees 2,509 emails between July 12, 2012 and July 1, 2013 including frequent instances of many emails received in the same minute, Mees's counsel argues that, *"Without producing the emails in their original native format, with their exact electronic time stamps, it cannot be established whether Plaintiff truly sent over 3,000 emails in one year (or with the frequency that Buiter alleges)"*. Plaintiff's Memorandum of Law in Opposition to Defendant's Motion to Dismiss, p.9.

12. My counsel retained Omnivere, LLC. Collin Bentley, a computer forensics expert at Omnivere, asked me to identify and provide access to all devices and authorization for access to all service providers from which native file format copies of e-mail communications received from or sent to Mees may be retrieved. One of these devices, a Samsung 740U laptop, had to be retrieved from my apartment in London. Once that laptop was retrieved I provided Collin Bentley my iMac, Dell XPS laptop, Samsung 740U laptop, Blackberry Bold 9700, iphone 5, and Sandisk USB Thumb Drive, each of which was considered a potential source of native file format copies of e-mail communications received from or sent to Mees. I also provided Mr.


Bentley authorization to access to my BTInternet and Gmail email accounts and my Verizon Online Backup and Sharing account.

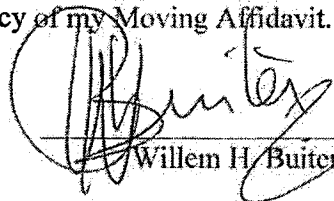
13. I am advised by Mr. Bentley, who will also submit an affidavit, that Verizon is currently unable to provide the necessary access to enable Mr. Bentley to download back-up data from my Verizon Online Backup and Sharing account, but that analysis of native format emails on the devices I provided Mr. Bentley with their exact electronic time stamps, reveals that I frequently received many emails from Mees within the same minute and that the total number of emails I received from Mees between July 12, 2012 and July 1, 2013 was at least 2,509.

14. I inadvertently misstated the number of emails I received from Mees between July 12, 2012 and July 1, 2013, and for that I apologize to the Court. As mentioned above, it seemed to me that I received more than 3,000 emails from Mees between July 12, 2012 and July 1, 2013. Using Microsoft Windows' "Replace" option in the "Replace or Skip Files" dialog box I tried to remove any duplicate Microsoft Outlook (email) files stored on my three computers before I copied the email files into a pdf, and I thought I had done so. Contrary to Mees' counsel's suggestion, I had no reason to inflate the number of emails I received from Mees between July 12, 2012 and July 1, 2013 from at least 2,509 to over 3,000, as this difference is immaterial; such a difference does not change the fact that Mees's emails to me, both in number and in content, demonstrate a pattern of continued harassment.

15. In all other respects, I reaffirm the accuracy of my Moving Affidavit.

Sworn to before me this
21 day of April, 2015


Notary Public


Willem H. Buiter



BOIES, SCHILLER & FLEXNER LLP

333 MAIN STREET • ARMONK, NY 10504 • PH. 914.749.8200 • FAX 914.749.8300

October 20, 2014

BY MAIL

Samantha Schott, Esq.
Assistant District Attorney
New York County District Attorney's Office
One Hogan Place
New York, New York 10013

Re: *People v. Heleen Mees*, Dkt. # 2013NY050589 (N.Y.C. Crim. Ct.)

Dear Ms. Schott:

We represent the defendant, Dr. Heleen Mees ("Mees"), in the above-captioned matter, in which we have appeared as co-counsel with Ira London, Esq. We write to raise a matter of grave concern and request that you take immediate action to investigate certain screenshots that our client's accuser, Mr. Willem Buiter ("Buiter"), took of her. As you are aware, the July 1, 2013 criminal harassment and stalking complaint against our client alleges that Mees sent Buiter "naked pictures of herself masturbating," and that this caused Buiter "severe annoyance and alarm." As you know from the documents in your possession, there is no record of any such naked pictures. In addition, on February 4, 2014, we showed you an email, in which Buiter, responding to a nude picture of another woman, stated that "pictures like that of yourself are always welcome" (*see* Exhibit A). Accordingly, Buiter's claim that he was severely annoyed by naked pictures from Mees is false.

We contact you concerning this issue once again because we recently made the alarming discovery that during the course of their consensual sexual relationship, Buiter secretly and without Mees' consent took approximately *1,252 screenshots* of their Skype sex sessions and saved those screenshots on his computer (presumably for his future enjoyment). We are examining if this surreptitious recording of Mees' intimate parts without her permission and against her explicit wishes might qualify as a felony (Penal Law § 250.45; *People v. Schreier*, 22 N.Y.3d 494 (2014)).

Buiter's secret recording of the parties' intimate love play is particularly alarming because Buiter has advised us that he provided these records to you to support his accusations of harassment. Since your decision to prosecute this case thus appears to have been based, in part, on these materials, we request that you obtain from Buiter electronic copies of the screenshots in their native format in order to determine that the screenshots were taken from *his*, not Mees' computer. Such a simple investigation on your part will conclusively demonstrate that Buiter was voluntarily on Skype and took his jolly good time to ensure he made extensive records of it for his personal pleasure. He

BOIES, SCHILLER & FLEXNER LLP

Samantha Schott, Esq.

October 20, 2014

Page 2

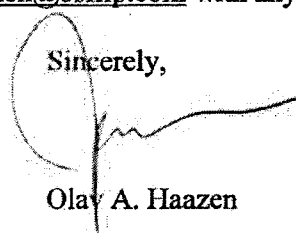
thus *cannot* have been annoyed. As anyone knows, an unwelcome Skype video call may be terminated with a simple push on the "End Call" button; no one can be forced to go onto Skype and "undergo" the viewing of sexual activity.

We further request that you review the metadata to determine *when* the screenshots were taken. If the metadata reveal that they were taken in 2013, this would prove that Buiter was voluntarily taking part in Skype sex with Mees up to the very end. If the screenshots were taken in 2011 or 2012, they show that Buiter severely misled the District Attorney's Office when he told you that he only had a brief physical relationship with Mees (which started in 2008) and that he had been telling Mees "[s]ince November 7, 2009" to cease any contact. Either way, after all that has been done to our client's life and career, we believe it is your responsibility to perform this very basic and simple investigation.

We note that it is Buiter's assertion that *Mees* somehow took these screenshots (even though in each frame both her hands are visibly otherwise occupied) and emailed them to him, and that they were in some inexplicable fashion *accidentally* saved on his computer. This story clearly is nonsensical. It is very difficult to email 1,252 picture files; if Mees wanted to send sexual material like this, it would have been much easier to send a few short video files rather than 1,252 stills of the same activity. Of course, if Mees really emailed Buiter the screenshots, Buiter should produce those emails. Indeed, please request that he do so, and you will find out that he is unable to produce such emails *because they do not exist*.

Accordingly, we request that you ask Buiter to produce both the screenshots in their native format and Mees' purported emails forwarding them to Buiter, review them, and advise us of your findings. We greatly appreciate your cooperation. Please feel free to contact me at (914) 749-8200 or ohaazen@bsflp.com with any questions.

Sincerely,



Olay A. Haazen

Copy:

Ira D. London, Esq.

EXHIBIT E

BOIES, SCHILLER & FLEXNER LLP

333 MAIN STREET* ARMONK, NY 10504* 914-749-8200* FAX 914-749-8300

October 28, 2014

Cyrus R. Vance, Jr., District Attorney
The New York County District Attorney's Office
One Hogan Place
New York, New York 10013

Re: *The People of the State of New York v. Heleen Mees*,
No. 2013NY050589 (N.Y.C. Crim. Ct.)

Dear Mr. Vance:

We represent Dr. Heleen Mees, a former New York University economics professor, political commentator, lobbyist, and public figure in her country of origin, the Netherlands, who is being prosecuted by your Office for second-degree menacing, third- and fourth-degree stalking, second-degree harassment, and second-degree aggravated harassment. *See* Pen. L. §§ 120.14(2), 120.45(2), 120.50(3), 240.26, and 240.30(1)(a). We write to advise you that further prosecution of this matter would be unconstitutional and a violation of international law. We have also discovered new evidence that suggests that the purported "victim" dramatically misled your Office and may have fabricated and tampered with evidence. We respectfully request that you exercise your prosecutorial discretion to withdraw all misdemeanor charges and immediately terminate the prosecution of our client, without unnecessary motion practice. We do so for three reasons.¹

First, all but three of the factual allegations against our client concern pure speech acts of the kind that the Court of Appeals has now definitively held are protected by the state and federal constitutions, and cannot be criminalized or prosecuted. Whatever the state of the law prior to the Court of Appeals' rulings, the People are now on notice that the continued prosecution for Mees' acts of pure speech is improper.²

Second, two of the three additional factual allegations involve conduct in foreign nations, to wit alleged attempted encounters in the Netherlands and China. These extraterritorial acts not only fall outside your Office's prosecutorial jurisdiction, they were, in fact, *legal* in the jurisdictions where they were allegedly committed. To prosecute our client for such acts is a violation of international law, as well as federal and state law, including well-established conflict

¹ While this matter was adjourned for 1 year in contemplation of dismissal on March 10, 2014, our client continues to suffer the severe consequences of the pendency of this case, including because her accuser continues to make false accusations about her, which create the risk that the active prosecution could be reopened. *See infra*, § II.

² The statutes are also unconstitutional *as applied*: the communications for which our client, a lobbyist and political commentator, is prosecuted contain at least 30 acts of political speech in its purest form. *See Ex. 1*.

Cyrus R. Vance, Esq.
 October 28, 2014
 Page 2 of 17

of law rules. (The third non-speech allegation is on triple-hearsay, which has no place in an Information).

Third, as we previously demonstrated to Assistant District Attorney Samantha Schott, the criminal complaint and the accusatory instrument are riddled with false statements by the accuser, Prof. Willem Buiter. His credibility is now so shattered that the prosecution cannot win this case at trial. While the falsehoods were sufficient reason for your Office to offer the ACD, Ms. Schott refuses to drop the charges altogether—even though we advised her of significant *additional* exculpatory evidence *after* the ACD was entered, including an email showing that the encounter in China was, in fact, pre-arranged and evidence that the nude photos that Mees supposedly sent were in reality screenshots that *Buiter* took of Skype calls in which he voluntarily participated. We refer to additional instances where the accuser demonstrably misled your Office and fabricated incriminating evidence in § V below.

Because the People appear to have been misled into prosecuting this case (and the police into arresting our client) by a slew of false and misleading statements by the accuser, we fail to see why your Office would want to proceed with this case. The People gain very little by keeping this matter open until March 9, 2015 or insisting on the ACD. Mees completed all 14 counseling sessions that your Office believed desirable and the Court imposed. She also has absolutely no intention of contacting the accuser ever again. What is left is a classic obey-the-law injunction. Such injunctions are generally recognized to have limited utility because they “do not require the defendants to do anything more than that already imposed by law.” *Rowe v. N.Y. State Div. of the Budget*, 2012 WL 4092856, at *7 (N.D.N.Y. Sept. 17, 2012).

I. Background

Our client, then-professor Heleen Mees, was arrested and charged with various counts of stalking and harassment on July 1, 2013, based on a complaint by fellow economics professor and chief economist of Citigroup, Willem Buiter. *See Ex. 2*. Buiter apparently told the police that the two of them once had a short relationship and that Mees has since stalked and harassed him for several years. *Ex. 3* at 2. Buiter apparently did not advise the police, or your Office, that in reality their consensual sexual relationship had lasted *four* years, and that the two had only *recently* broken up. He claimed that Mees had harassed him by sending thousands of emails (*Ex. 2* at 2; *Ex. 3* at 2), but omitted that Mees’ emails were part of the regular email exchange between the two lovers during those years, during which Buiter also sent Mees some 1,000 messages. He apparently also did not tell the police that he had only just moved to New York City, and that everything that allegedly occurred in the years preceding his move, including the bulk of the email exchanges, occurred in other countries before Buiter had any connection whatsoever with New York. Buiter represented that Mees also harassed his children by email, and that he feared for their safety. *Ex. 2* at 2. He apparently did not advise the police or your Office that his “children” are, in fact, grown-ups in their twenties, who do not live, and never lived, in the State of New York, and that Mees never met them, or sent them even a *single* email.

The Information that ADA Schott issued on August 5, 2013, charges Mees with five misdemeanors based on three categories of allegations:

Cyrus R. Vance, Esq.
October 28, 2014
Page 3 of 17

- (i) allegations that Mees sent Buiter 3,000 emails in four years, and 164 Facebook messages, and that she called his cell phone hundreds of times (the “**Speech Act Allegations**”);
- (ii) allegations that the content of certain messages was annoying and threatening, including sexually explicit messages (“Shall I lick your b---s?”), emails asking if he would “meet her for a drink,” artwork of two little dead birds, an angry email stating “I hope you die,” and a message after Buiter’s flight to London took off “I hope your plane falls from the sky”—a message she retracted five minutes later and Buiter *cannot* have read until he landed on foreign soil (the “**Speech Content Allegations**”); and
- (iii) allegations that in “May 2010, the defendant tried to meet with [Buiter] at [his] hotel in Beijing, China,” that “in January 2013, the defendant tried to meet [him] at [his] hotel in Amsterdam, The Netherlands, by using a fake name,” and that on “May 6, 2013, the defendant came to [Buiter’s] apartment building in the County and State of New York, and tried to be let up . . .” (the “**Conduct Allegations**”).

Ex. 3 at 2.

On February 4, 2014, counsel met with ADA Schott and her supervisor, Jeanine Launay, to walk them through documentary evidence showing significant falsehoods in Buiter’s statements in the July 1 complaint and August 5 Information, and the details of Buiter’s four-year relationship with Mees, the frequent initiative *Buiter* took to contact Mees, and his own sexually explicit messages. Following that meeting, your Office offered Mees a one-year ACD. Eager to avoid a public trial, primarily for financial reasons and to avoid further reputational and emotional harm, Mees consented to the ACD, which was entered by Justice Steven Statsinger on March 10, 2014.

II. The Continuing Threat of Prosecution and Enduring Effects on Mees

Since the ACD, Mees has continued to suffer the consequences of her arrest and prosecution, and she continues to live under a threat of further prosecution. In fact, the past months have shown that the particularities of this case—an accuser engaged in *continuing* false statements and a public figure whose arrest and prosecution became a veritable media hype—prevent Mees from enjoying the benefits normally associated with ACDs.

The purpose of an ACD is “to provide a shield against the criminal stigma” that would otherwise attach to a defendant. *Lancaster v. Kindor*, 471 N.Y.S.2d 573, 579 (1st Dep’t 1984); accord *Smith v. Bank of Am. Corp.*, 865 F. Supp. 2d 298, 302 (E.D.N.Y. 2012) (Weinstein, J.) (ACD designed to avoid persons charged with minor offenses being permanently designated as criminals). When granted an ACD, a defendant “is ‘entitled to the full benefit of the record sealing and expunging provisions’ that attend an acquittal.” *Rothstein v. Carriere*, 373 F.3d 275, 287 (2d Cir. 2004) (quoting *Hollender v. Trump Village Co-op, Inc.*, 58 N.Y.2d 420 (1983)). The defendant shall be restored “to the status he occupied before his arrest and prosecution.”

Cyrus R. Vance, Esq.
October 28, 2014
Page 4 of 17

CPL § 170.55(8). The ACD statute specifically provides that “[n]o person shall suffer any disability as a result” of an ACD. *Id.* “The over-all effect of a consummated ACOD dismissal is then to treat the charge *as though it never had been brought.*” *Hollender*, 58 N.Y.2d at 425 (emphasis added).

Our client will likely be deprived of all the above benefits to which she is supposed to be entitled. She lost her NYU professorship, her job as a newspaper columnist, and all of her lobbying and consulting business. While the courts recognize that the “ability to earn a living is an important factor in avoiding criminality” through an ACD, *Smith*, 865 F. Supp. 2d at 300, the public airing of Mees’ private and intimate conversation with Buiter and the public ridicule that followed her arrest and prosecution make it virtually impossible for her to earn a living as an economics professor, political lobbyist, commentator, or public speaker. She clearly suffers, and will continue to suffer, a “disability as a result” of the prosecution. Because the news of her arrest and prosecution was reported around the globe and every detail of the accusations against her is preserved on hundreds of websites, this ACD is not sufficient to return her to a state as though the prosecution “never had been brought.” The “full benefit” of sealing and expunging the record will hardly make Mees’ arrest and prosecution a “nullity.” Nor is the ACD in any way sufficient to restore her previous status.

These consequences are understandable, and could even be justifiable, if Mees’ actions, here and abroad, could actually be prosecuted here, and if the statements that Buiter “spiced up” in order to convince the police and your Office and to entice the media around the world, were true. But for the reasons below, this is *not* the case.

III. Continued Prosecution of Mees for Her Pure Speech Acts Is Improper.

Our client cannot, and should not, be subjected to these consequences on account of what are acts of protected speech (the **Speech Act Allegations** and the **Speech Content Allegations**). As you are aware, earlier this year, the Court of Appeals struck down the second-degree aggravated harassment statute (Pen. L. § 240.30(1)(a)) as unconstitutional under both the state and federal constitutions. *See People v. Golb*, 991 N.Y.S.2d 792 (2014). The court held that the criminalization of communicating with “intent to annoy” another person is a “proscription of pure speech” that goes beyond the constitutionally necessary limitations to “words which, by their utterance alone, inflict injury or tend naturally to evoke immediate violence.” *Id.* (quoting *People v. Dietze*, 75 N.Y.2d 47 (1989)). It also held that it is unconstitutionally vague and overbroad to prohibit communicating “in a manner likely to cause annoyance or alarm” to another person. *Id.* (quoting *People v. Dupont*, 486 N.Y.S.2d 169 (1st Dep’t 1985)). Thus, speech cannot constitutionally be prohibited just because it is annoying, whether the speech acts are, or are intended to be, annoying because of their content or their quantity and frequency.

A. The Stalking, Harassment, and Menacing Statutes At Issue Here Are Unconstitutional on Their Face.

The ruling in *Golb* affects all five statutes under which our client is prosecuted. Section 240.30(1)(a) (aggravated second-degree harassment) is unconstitutional on its face because it

Cyrus R. Vance, Esq.
 October 28, 2014
 Page 5 of 17

criminalizes communicating with “intent to annoy” another person, and thus proscribes pure speech in a manner that goes beyond the constitutionally necessary limitations to “words which, by their utterance alone, inflict injury or tend naturally to evoke immediate violence.” *Golb*, 991 N.Y.S.2d at 800; *accord People v. Marquan M.*, 24 N.Y.3d 1 (2014) (cyberbullying statute unconstitutional on its face because it broadly prohibited all communications that are meant to harass or annoy a person).

By the same token, Sections 240.26(3) (second-degree harassment), 120.50(3) (third-degree stalking), 120.45(2) (fourth-degree stalking), and 120.14(2) (menacing)—all of which are capable of encompassing protected speech—are unconstitutionally vague and overbroad. With the exception of Section 120.45(2), *none* of these statutes limit themselves to speech acts that “by their utterance alone, inflict injury. . .” Sections 240.26(3) and 120.50(3) both criminalize an “annoying course of conduct” that a defendant engages in “with intent to harass, annoy or alarm” another person, if the conduct serves “no legitimate purpose” (§ 240.26(3)) or “is likely to cause reasonable fear of injury” (§ 120.50(3)). Section 120.45(2) similarly criminalizes communicating with a person or his family if these communications serve “no legitimate purpose” and also cause material mental or emotional harm, and Section 120.14(2) criminalizes engaging in a course of conduct “intentionally placing another person in reasonable fear of injury.” The case law is clear that in order to pass constitutional muster, criminal prohibitions must carve out constitutionally protected speech from the conduct or speech that their broad language otherwise would cover. *See Dietze*, 75 N.Y.2d at 50 (even when certain conduct could be proscribed without violating the Constitution, on their face, these statutes prohibit “a substantial amount of constitutionally protected expression,” which requires that they be stricken); *People v. Pierre-Louis*, 927 N.Y.S.2d 592, 595-97 (Dist. Ct. Nassau Cnty. 2011) (vagueness and overbreadth of statute that fails to distinguish between protected versus unprotected speech is “readily apparent”).

None of the above statutes, however, provides for a valid carve-out. *None* of the qualifiers that these statutes added—that the communication is prohibited only if it is without legitimate purpose or threatens someone with injury—are sufficient to salvage these prohibitions of speech from constitutional infirmity. As the Court of Appeals made clear in *Marquan* earlier this year, “the First Amendment *forbids* the government from deciding whether protected speech qualifies as ‘legitimate . . .’” *Marquan*, 24 N.Y.3d at 7 (emphasis added); *accord Simon & Schuster, Inc. v. Members of the N.Y.S. Crime Victims Bd.*, 502 U.S. 105, 116 (1991) (“Regulations which permit the Government to discriminate on the basis of the content of the message cannot be tolerated under the First Amendment.”). Because of this overbreadth, each of these statutes is capable of covering (and, in fact, covers) speech acts that *cannot* constitutionally be proscribed, including purely political or potentially annoying yet non-threatening speech.

B. The Stalking, Harassment, and Menacing Statutes At Issue Here Are Also Unconstitutional As Applied.

State and federal precedents make clear that continuing this prosecution under the specific circumstances of this case would be unconstitutional. Because the U.S. and New York Constitutions do not permit any proscription of pure speech beyond “words which, by their utterance alone, inflict injury or tend naturally to evoke immediate violence,” *Golb*, 991

Cyrus R. Vance, Esq.
 October 28, 2014
 Page 6 of 17

N.Y.S.2d at 800, the **Speech Content Allegations** and the **Speech Act Allegations** at issue here would, at a minimum, need to have amounted to *threats*. Clearly, they do not.

1. *The Speech Content Allegations*

A proscribable “true threat” requires “a serious expression of an intent to *commit* an act of *unlawful violence*.” *People v. Bonitto*, 777 N.Y.S.2d 900, 902 (N.Y.C. Crim. Ct. 2004) (emphasis added) (quoting *Virginia v. Black*, 538 U.S. 343, 359 (2003)); *accord Vives v. City of N.Y.*, 305 F. Supp. 2d 289, 298-99 (S.D.N.Y. 2003). Thus, stating to an abortion clinic doctor after the murder of another doctor “I hope you’re next” is not constitutionally proscribable because it is not a true threat of any immediate action by the speaker himself. *New York v. Operation Rescue National*, 273 F.3d 184, 196-97 & n. 5 (2d Cir. 2001). By the same token, statements like “I hope you die” or “I hope your plane falls from the sky,” sending artwork of dead birds, or even tweeting to the world (from Austin, Texas) that one is a “natural” at the shooting range—even if those statements could have the meaning that Buiter claims he thought they had—are not true threats. Wishing someone bad fortune or even death cannot constitutionally be considered a crime because these are not direct threats of some specific action that the speaker intends to do.³

Even actual threats directed at the victim, and those made “in a very menacing manner,” *People v. Digianni*, 2010 WL 1542527, at *5 (Just. Ct. New Castle March 11, 2010), cannot be criminally proscribed unless the threat is *imminent*. *Chaplinsky v. New Hampshire*, 315 U.S. 568, 572 (1942) (speech must have tendency “to incite an immediate breach of the peace”); *New York ex rel. Spitzer v. Cain*, 418 F. Supp. 2d 457, 477 (S.D.N.Y. 2006) (statements like “Go to hell” and “I’d like to stick a coat hanger in you” do not “indicate the unequivocal immediacy and express intention of a true threat”); *Dietze*, 75 N.Y.2d at 51-53 (first-degree harassment charge dismissed because threat to “beat the crap out of [the complainant] some day or night on the street” does not create an imminent danger of violence, and thus does not fall within the scope of constitutionally proscribable speech).⁴

Threats must also be unequivocal and specific. *Behlin*, 863 N.Y.S.2d at 365-66 (defendant’s threat that he “was going to get her” and she should better “watch it” not specific as to the harm, time or place, and therefore not harassment); *Digianni*, 2010 WL 1542527, at *5, *7

³ *Accord People v. Khaimov*, 906 N.Y.S.2d 782 (N.Y.C. Crim. Ct. 2009) (warning to “[w]atch your step or something serious is going to happen to you,” stating no specific harm, time or place of occurrence, is not unequivocally threatening); *People v. Bender*, 2007 WL 258290, at *4 (N.Y.C. Crim. Ct. Jan. 31, 2007) (without threats of violence or harm, rude or angry words are not enough to constitute aggravated harassment) (quoting *People v. Webers*, 808 N.Y.S.2d 920 (1st Dep’t 2005)); *Pierre-Louis*, 927 N.Y.S.2d at 595 (“I’m coming at you with fury” too vague to be a true threat).

⁴ See also *People v. Behlin*, 863 N.Y.S.2d 362, 366 (N.Y.C. Crim. Ct. 2008) (actionable threats require “immediacy,” i.e. some “ultimatum threatening a specific type of harm which would befall the complainant at a predetermined time or place in the near future”); *People v. Limage*, 851 N.Y.S.2d 852, 856 (N.Y.C. Crim. Ct. 2008) (actionable threats require a “sense of imminence, rather than some abstract notion of what might happen at an unspecified later time”).

Cyrus R. Vance, Esq.
 October 28, 2014
 Page 7 of 17

(phone message “I’m going to get you,” not in close proximity to the victim or with knowledge of the victim’s whereabouts lacked requisite “sense of imminence”); *accord People v. Yablov*, 706 N.Y.S.2d 591, 595-96 (N.Y.C. Crim. Ct. 2000) (“we’ll get you”).

Under these precedents, the **Speech Content Allegations** do not suggests any proscribable true threats. In light of countless examples in the case law that held insufficiently threatening far more serious statements like “I will beat the crap out of you” (*Dietze*), “I’d like to stick a coat hanger in you” (*Cain*), and “we’ll get you” (*Yablov*), there is no chance that a judge (or, if necessary, a jury) will find Mees wishing Buiter misfortune (including a message she had retracted before Buiter even read it) threatening speech.⁵ Angry expressions of the drop-dead and go-to-hell type are not threats. The fact that Mees emailed these statements, rather than telling Buiter face-to-face, and the dates of her purported “death wishes”—September 14-15, 2012, *i.e.* long before Buiter moved to New York—conclusively establish that there was no imminence or proximity either in time or place. The idea that Buiter, a hyper-intelligent and level-headed man, *genuinely* believed that a 43-year old economics scholar from Brooklyn would have the capability of making planes “fall from the sky” is ludicrous.

The sexual explicitness of Mees’ messages—in a tone comparable to Buiter’s own profanity toward Mees (*see Ex. 5*)—and images of nude women—about which Buiter commented to Mees “Pictures like that of yourself are always welcome” (*Ex. 6*)—cannot possibly be grounds for prosecution in the absence of any threat. *See Dietze*, 75 N.Y.2d at 51 (unless speech presents a clear and present danger of some serious substantive evil, even provocative and vulgar speech “may neither be forbidden nor penalized”); *Bonitto*, 777 N.Y.S.2d at 90-3 (a prisoner’s letter from his prison address to a random person, requesting contact and a response and stating he hoped he “may get lucky,” but without any threat of violence was, while “unsettling,” “incapable of constituting a true threat, as a matter of law” and did not amount to either harassment or a threat).

2. The Speech Act Allegations

The **Speech Act Allegations**, which accuse our client of sending 3,000 emails in four years, sending 164 Facebook messages, and making hundreds of unanswered cell phone calls, cannot form the basis of Mees’ further prosecution. It is obvious that constitutionally protected speech does not lose its protection just because a person chooses to exercise his or her constitutional right with high frequency. *See Yablov*, 706 N.Y.S.2d at 596 (“[V]olume of telephone calls alone does not constitute a violation of [Section 240.26].”). *Without a specific threat*, even a barrage of messages cannot constitutionally be proscribed as harassment or aggravated harassment. *Id.* at 595-6; *see Bender*, 2007 WL 258290, at *4 (without threats of violence or harm, no aggravated harassment).

⁵ Whether a communication is a true threat rather than protected speech is “a threshold question of law for the court.” *Behlin*, 863 N.Y.S.2d at 365 n. 1; *accord People v. Thompson*, 905 N.Y.S.2d 449, 496 (N.Y.C. Crim. Ct. 2010). Mees’ “I hope you die” email is no worse than what Buiter had to say to Mees: “Life sucks, then you die.” *See Ex. 4*.

Cyrus R. Vance, Esq.
 October 28, 2014
 Page 8 of 17

This is, of course, most obvious for the “hundreds” unanswered phone calls Mees allegedly made to Buiter. Unanswered phone calls cannot be threats, as they cannot, by definition, have a threatening content (or any content at all). *Yablov*, 706 N.Y.S.2d at 595 (no second-degree aggravated harassment where defendant called 22 times but left no messages and thus made no specific threat). Such phone calls also cannot form the basis of a second-degree harassment (§ 240.26(3)) or fourth-degree stalking (§ 120.45(2)) charge because both of these misdemeanors require that the Information provide factual allegations from which to discern *the absence of a legitimate purpose* as a necessary element of the charges. See *People v. Goris*, 975 N.Y.S.2d 368 (N.Y.C. Crim. Ct. 2013). Allegations of phone calls that were not completed and therefore have no content do not show on their face for what purpose the defendant was trying to speak with the person. By definition, they “do not demonstrate that the communication was made with lack of legitimate purpose.” *Id.*

The same rationale applies to the 3,000 emails and 164 Facebook messages Mees allegedly sent. Criminalization of speech acts based solely on their volume, without regard to content, is plainly overbroad, as it indiscriminately lumps together both protected and unprotected speech. *Pierre-Louis*, 927 N.Y.S.2d at 595-97. There may be no better example of the impropriety of that approach than the case at bar. Mees is a political and economic commentator, who frequently engaged in political discussion with Buiter, including during the 2009-2013 period. A sampling of pure political speech that was part of the volume of communications that your Office has included as predicate acts is attached as **Ex. 1**.⁶ Prosecuting Mees for the totality of her communications with Buiter necessarily penalizes her for engaging in such pure political speech. See *People v. Mangano*, 100 N.Y.2d 569, 571 (2003) (repeated messages that include complaints about government actions, no matter how harassing, crude, or offensive, do not fall “within any of the proscribable class of speech or conduct”).

3. *Re-characterizing Speech Acts as “Conduct” Does Not Make this Prosecution Constitutional.*

We are aware that Sections 240.26(3) (second-degree harassment), 120.50(3) (third-degree stalking), and 120.14(2) (menacing) all purport to criminalize a “course of conduct,” not specifically communications, and that several courts, including the Court of Appeals and Justice Statsinger, have upheld similar statutes on a theory that threatening conduct is not protected speech. See *People v. Shack*, 86 N.Y.2d 529 (1995); *People v. Seitz*, 2014 WL 4358402, at *3 (N.Y.C. Crim. Ct. Sept. 4, 2014) (Statsinger, J.) (distinguishing impermissible prohibition of pure speech from permissible criminalization of conduct, of which speech may be a component) (citing *Shack*). But *Seitz* was plainly wrongly decided. Whether the government labels its prosecution of constitutionally protected speech as the criminalization of “conduct” or “speech” is irrelevant. A statute is overbroad as long as its prohibition of “conduct” reaches

⁶ See, e.g., Email dated November 26, 2012 (Mees’ political column regarding debt forgiveness), December 9, 2012 (Mees’ column regarding the innovation crisis), December 13, 2012 (Mees’ Financial Times blog post regarding economic growth), December 17, 2012 (column regarding gun control in U.S. politics), January 31, 2013 (Financial Times blog regarding Fitch), February 23, 2013 (draft New York Times OpEd piece regarding low yields and large bubbles), March 1, 2013 (Financial Times blog post regarding interest rates), April 7, 2013 (requesting Buiter’s comments on column on housing bubbles), April 9, 2013 (Project Syndicate blog post regarding transatlantic strife).

Cyrus R. Vance, Esq.
 October 28, 2014
 Page 9 of 17

constitutionally protected speech, such as the making of phone calls or sending unwanted mail. *See Mangano*, 100 N.Y.2d at 571; *Vives*, 305 F. Supp. 2d at 301 (criticizing New York police and prosecutors for continuing to arrest and prosecute people “for engaging in *conduct* that is firmly protected by the First Amendment”) (emphasis added); *Thompson*, 905 N.Y.S.2d at 459 (statutory reference to proscribed “conduct” sufficient to cover certain types of speech).

Shack does not survive the Court of Appeals’ recent holding in *Marquan*, which held an anti-bullying statute unconstitutional because it was *capable* of covering acts of pure speech. *Marquan*, 24 N.Y.3d at 6, 8. In *Shack*, the Court of Appeals held that Section 240.30(2) (second-degree aggravated harassment) does not unconstitutionally reach protected speech because its reference to “conduct” expressly excludes such speech by making an exception for telephone calls for the “purpose of legitimate communication.” 86 N.Y.2d at 533, 535; *id.* at 537. That reasoning no longer works, however, because the Court of Appeals no longer considers it permissible to use such a carve-out to save the statute from constitutional infirmity. *Marquan*, 24 N.Y.3d at 7 (“the First Amendment *forbids* the government from deciding whether protected speech qualifies as ‘legitimate . . .’”) (emphasis added).⁷

Now that the practice of prosecuting people for speech that is annoying (*Golb*), serves “no legitimate purpose” (*Marquan*), or consists of high-volume repetitive messages that contain government criticism (*Mangano*) have been declared unconstitutional, the only appropriate course of action is to discontinue this prosecution. We see no reason why your Office, having been misled into prosecuting this case, would want to ratify Buiter’s actions and, having been advised of its constitutional and factual infirmity in light of pre-existing law, make its own independent decision to continue to prosecute this matter.

IV. The Exercise of Extraterritorial Jurisdiction in this Case Violates State, Federal, and International Law.

A second reason why the continued prosecution of our client is inappropriate is the extraterritorial nature of the conduct on which the **Conduct Allegations** are based. The Information alleges that in January 2013, Mees tried to meet with Buiter in his hotel in Amsterdam, the Netherlands, and that three years earlier, in 2010, she had done the same in

⁷ Similarly, *Shack*’s alternative rationale does not survive the Court of Appeals’ decision in *Golb*. *Shack* held that a telephone is like a mailbox and that people should be able to refuse unwanted mail from trespassers delivering it to their homes. 86 N.Y.2d at 535-36. Unlike the delivery of unwanted mail to “a private place” (*id.*), however, calling someone, leaving voice or text messages, and sending emails are *not* a form of trespass. *See Pierre-Louis*, 927 N.Y.S.2d at 597 (“[M]aking a phone call, even uninvited to an individual is not a trespass.”). The *Golb* Court cited with approval Judge Scheindlin’s decision in *Vives v. City of N.Y.*, 305 F. Supp. 2d 289 (S.D.N.Y. 2003); *see Golb*, 991 N.Y.S.2d at 800. *Vives* recognized that Americans in the Information Age are “bombarded daily” with large volumes of annoying communications, including “email boxes filled with spam” and “prerecorded advertisements left on telephone answering machines.” 305 F. Supp. 2d at 292-93. Neither the fact that such communications annoy and/or alarm the recipients, nor that they are intended to do so, “can be a basis for arresting or prosecuting” anyone (*id.* at 299)—under a trespass theory or otherwise.

Cyrus R. Vance, Esq.
 October 28, 2014
 Page 10 of 17

Beijing, China.⁸ It is undisputed that Mees is a Dutch national, and that in January 2013, Buiter lived in London and that he did not move to New York until mid-February or later. Thus, it is clear that your Office is prosecuting a Dutch national for conduct that allegedly occurred in her own country, as well as in China, where that conduct is not prohibited, while the victim was not even a New York resident. The continued exercise of extraterritorial prosecutorial jurisdiction is highly improper and, in fact, violates well-established state, federal, and international law.⁹

A. The Present Prosecution for Extraterritorial Conduct Violates State Law.

The DA's Office has no authority to prosecute Mees for any acts allegedly committed in the Kingdom of the Netherlands or the People's Republic of China because those acts fall outside New York's power to prescribe. *See People v. McLaughlin*, 80 N.Y.2d 466, 471 (1992) ("Because the State only has power to enact and enforce criminal laws within its territorial borders, there can be no criminal offense unless it has territorial jurisdiction."); RESTATEMENT (THIRD) OF FOREIGN RELATIONS § 432 (1) ("A state may enforce its criminal law within its own territory through the use of police, investigative agencies, public prosecutors, courts, and custodial facilities, provided (a) the law being enforced is within the state's jurisdiction to prescribe . . ."). As a fundamental principle of New York law, New York does not criminalize acts that occur abroad. McKinney's Statutes § 149 ("The laws of one state can have no force and effect in the territorial limits of another jurisdiction, in the absence of the consent of the latter."); *Western Transp. & Coal Co. of Mich. v. Kilderhouse*, 87 N.Y. 430, 435 (1882) ("It is very well settled that penal laws have no extra-territorial force."); *see also* RESTATEMENT (FIRST) OF CONFLICT OF LAWS § 425 ("Except as stated in § 426 [acts by U.S. national, on U.S. vessel, or in territorial waters], a state has no jurisdiction to make an act or event a crime if the act is done or the event happens outside its territory.").

⁸ On their face, these allegations of conduct 3 years apart cannot form the predicates for the "course of conduct" charges pursuant to Sections 120.14(2), 120.50(3), 120.45(2), and 240.26(3). *See People v. Webers*, 808 N.Y.S.2d 920 (1st Dep't 2005) (as a matter of law, 2 telephone calls over 4 months apart do not constitute "a course of conduct" under second-degree harassment statute); *People v. Bilus*, 804 N.Y.S.2d 670, 675 (Dist. Ct. Nassau Cnty. 2005) (2 visits to complainant's work address 6 months apart "do not constitute a course of conduct" for purpose of fourth-degree stalking).

⁹ The only other **Conduct Allegation**—that Mees showed up in Buiter's apartment building—is triple-hearsay. Mees was visiting the Consul General of her country, who happens to live in the same building (*see Ex. 7*)—a visit protected by Article 36 of the Vienna Convention on Consular Relations, 21 U.S.T. 77 (1963) (providing that "consular officers shall be free to communicate with [their] nationals" who "shall have the same freedom with respect to . . . access to consular officers"). Buiter (or Ms. Schott) appears to have misunderstood the he-said-she-said-he-said-she-said relay of communications. Buiter concedes in an affidavit submitted in related civil litigation that "on the night of May 6, 2013, . . . the doorman in the building in Manhattan where my wife and I live informed us that Mees . . . was asking to see us." (emphasis added). *Ex. 8* (excerpts from Buiter Affidavit) ¶ 27. Buiter's wife confirms that she was the one who spoke with the doorman. *Ex. 9* ("[T]he doorman at our apartment building informed me that Mees was in the lobby to see my husband and me.") (emphasis added). Because hearsay, and certainly triple hearsay, is unreliable and prone to give rise to misunderstandings such as these, New York requires that a misdemeanor Information be based on "[n]on-hearsay allegations." CPL § 100.40(1)(c); *accord People v. South*, 912 N.Y.S.2d 837, 840-41 (App. Term 2010) (finding facial insufficiency because "an information must allege nonhearsay facts"). This allegation thus has no place in the Information.

Cyrus R. Vance, Esq.
 October 28, 2014
 Page 11 of 17

While the legislature may create certain exceptions, it is “the settled rule of statutory interpretation, that unless *expressly* stated otherwise, ‘no legislation is presumed to be intended to operate outside the territorial jurisdiction of the state . . . enacting it.’” *Goshen v. Mut. Life Ins. Co. of N.Y.*, 730 N.Y.S.2d 46, 47 (1st Dep’t 2001) (citation omitted; emphasis added); *cf. Morrison v. Nat’l Australia Bank Ltd.*, 561 U.S. 247, 248 (2010) (“When a statute gives no clear indication of an extraterritorial application, it has none.”). There is nothing, let alone express language, in the harassment, menacing, and stalking statutes at issue here to suggest that the legislature intended to prescribe acts outside the territory of New York State or the United States.

Even if Sections 120 and 240 of the Penal Code did have an extraterritorial scope, as a matter of conflict of laws New York law has no application. Under well-established conflict rules, the law of the state where an act is done or event is caused determines whether the act or event is a crime. RESTATEMENT (FIRST) OF CONFLICT OF LAWS § 428(1). “A person is liable to punishment for a crime, therefore, only by the law of the state where the essential event takes place and only if the law of that state makes the event punishable.” *Id.* § 428 cmt. a. Here, the hotel visits allegedly occurred in the Netherlands and China, and so the respective criminal laws of these countries, *not* New York law, determine whether the acts constitute crimes.

We have solicited the opinions of experts from the Netherlands and China, and both have confirmed that the alleged hotel visits are not criminal offenses in their respective countries. *See Ex. 10* (Declaration of Hon. Willem Geelhoed) ¶ 3 (“The accusations against Dr. Mees—*i.e.* that she tried to meet with Prof. Buiter, tried to be let up to Prof. Buiter’s hotel room, and/or used a false name—do not, either jointly or in isolation, constitute a criminal offense under the criminal laws of the Netherlands, and do not violate any laws of the Netherlands.”); *Ex. 11* (Declaration of Chen Yun, Esq.) at 2 (“There is no provision in the Criminal Law of the People’s Republic of China or any criminal regulations of the City of Beijing that prohibits ‘stalking’ or ‘harassment.’ Nor is there any other criminal prohibition that even comes close to criminalization of the conduct . . . at issue here.”). Accordingly, the extraterritorial **Conduct Allegations** are an improper basis for this prosecution.

B. This Prosecution Violates Federal and International Law.

The continued prosecution of our client for acts she allegedly committed abroad also violates federal due process and international law. For extraterritorial application of a criminal statute to comport with due process “there must be a sufficient nexus between the defendant and the United States, so that such application would not be arbitrary or fundamentally unfair.” *United States v. Youssef*, 327 F.3d 56, 111 (2d Cir. 2003) (citation omitted); *accord United States v. Caicedo*, 47 F.3d 370, 372 (9th Cir. 1995). (“[P]unishing a crime committed on foreign soil . . . is an intrusion into the sovereign territory of another nation. As a matter of comity and fairness, such an intrusion should not be undertaken absent proof that there is a connection between the criminal conduct and the United States sufficient to justify the United States’ pursuit of its interests.”). Whether a sufficient nexus exists, is governed by well-established principles of international law, including the principles of international comity reflected in Sections 402 and 403 of the Restatement of Foreign Relations.

Cyrus R. Vance, Esq.
 October 28, 2014
 Page 12 of 17

As you know, “[i]nternational law is a part of our law and as such is the law of all States of the Union.” *Skiriotos v. State of Fla.*, 313 U.S. 69, 72-73 (1941); *accord Presbyterian Church of Sudan v. Talisman Energy, Inc.*, 374 F. Supp. 2d 331, 339 (S.D.N.Y. 2005) (international law “binding on all States”); RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 111 (1987) (“International law [is] supreme over the law of the several States.”). “Since international and other foreign relations law are the law of the United States, under the Supremacy Clause of the Constitution an exercise of jurisdiction by a State that contravenes the limitations of §§ 402-403 is invalid.” REST. (THIRD) OF FOREIGN REL. § 402 cmt. k.

Under international law, as codified in Section 402, there are only five bases for giving criminal statutes an extraterritorial scope—the universality principle, the nationality principle, the objective territorial principle, the protective principle, and the passive personality principle. *Youssef*, 327 F.3d at 91 n. 24; REST. (THIRD) OF FOREIGN REL. § 402 (1987). None of these grounds provides a basis for prosecution here.

The *universality principle* is limited to crimes so heinous as to be universally condemned by all civilized nations. It confers no jurisdiction over a lovers’ quarrel. The *nationality principle* applies only to acts committed abroad by U.S. citizens. *Matter of Garcia*, 802 F. Supp. 773, 780 (E.D.N.Y. 1992) (nationality principle has no application if defendant “is not a citizen, but only a resident alien”). It has no application here because Mees is not a U.S. citizen.

The *objective territorial principle* also can have no application here. It governs “[a]cts done outside a jurisdiction but intended to produce and producing detrimental effects within it.” *Strassheim v. Daily*, 221 U.S. 280, 285 (1911) (Holmes, J.). Thus, for New York to have geographical jurisdiction when conduct occurs outside of the state’s borders requires a result or effect within the state. See CPL § 20.20(2)(a)-(b). It is obvious, however, that Mees’ alleged 2010 visit to Buiter’s hotel in China had no effect in the State of New York or any U.S. territory. Buiter lived and worked in the United Kingdom at the time. He had lived there for 19 years, and did not move to New York until nearly three years later. Nor could Mees have *intended* a visit to her lover to have a substantial effect in the United States three years before he would move there. The same is true for the purported visit to his Amsterdam hotel in January 2013, at least a month and a half before Buiter even became a resident of this State. Neither the result nor any intended effect occurred in New York.

Similarly, the *protective principle*¹⁰ permits the criminalization or prosecution where out-of-state acts harm the State’s interests. See *Taub v. Altman*, 3 N.Y.3d 30, 34 (2004) (there must be a “concrete and identifiable injury” to either the county’s governmental processes or the welfare of the community); CPL § 20.10(4) (defining “particular effect” as “a materially harmful impact upon the governmental processes or community welfare” in the jurisdiction). Thus, in order for prosecutorial jurisdiction to lie, New York County must have suffered a materially harmful impact, “more than minor or incidental,” on “the well being of the community as a whole,” not merely a particular individual.” *Zimmerman*, 9 N.Y.3d at 425 (citation omitted);

¹⁰ Or “particular effect theory of geographical jurisdiction” (*People v. Zimmerman*, 9 N.Y.3d 421, 426 (2007); see CPL § 20.20(2)(b) (requiring an intent to cause “a particular effect in this state”)), also known in New York as the “injured forum principle” (*Steingut v. Gold*, 42 N.Y.2d 311, 321 (1977)).

Cyrus R. Vance, Esq.
October 28, 2014
Page 13 of 17

accord People v. Fea, 47 N.Y.2d 70, 76-77 (1979). In other words, the extraterritorial conduct must have “exposed a large number of county residents to a specific harm.” *Taub*, 3 N.Y.3d at 36.

No such interests are even remotely implicated here. Buiter and his wife were not residents of any county in the State, either in 2010 or in January 2013. Buiter’s children, who are British citizens, have never lived in the State of New York and are not part of this community. It would strain credulity to argue that the alleged hotel visits in the Netherlands and China—which obviously did not involve either Buiter’s wife or his children—even come close to having *any* impact, let alone a “materially harmful impact,” on the Manhattan “community as a whole.” *Zimmerman*, 9 N.Y.3d at 425. If there were any discernible effect, it would be minor and incidental, affecting no more than one or two particular individuals, who only later decided to become residents of New York.

The *passive personality* principle, which would permit a state to apply its criminal laws to an act committed by a non-citizen on foreign soil, “has not been generally accepted for ordinary torts or crimes,” and is only gaining acceptance “as applied to terrorist and other organized attack on a state’s nationals by reason of their nationality, or to assassination of a state diplomatic representatives or other officials.” REST. (THIRD) OF FOREIGN REL. § 402 cmt. g; *see id.* § 402(3) (“certain conduct outside its territory by persons not its nationals that is directed against the security of the state or against a limited class of other state interests”). We have found no cases suggesting that the passive personality principle has ever been accepted, or even invoked, in the state of New York. No New York court has so much as *mentioned* this principle, and no U.S. court, state or federal, has ever permitted the prosecution of a misdemeanor offense for any act allegedly committed on foreign soil based on the passive personality principle. *See* RESTATEMENT (SECOND) OF FOREIGN RELATIONS (1965) § 30(2) (“A state does not have jurisdiction to prescribe a rule of law attaching legal consequences to conduct of an alien outside its territory merely on the ground that the conduct affects one of its nationals.”); *id.* cmt. e (Subsection (2) of this Section rejects the so-called “passive personality” principle under which a number of states assert that they may prescribe rules governing the criminal conduct of aliens outside their territory if the victims of the crime are their nationals.”).

ADA Schott is criminally prosecuting a Dutch national for acts committed in her own country and China, where those acts are not a crime. This is particularly troubling because Buiter was at the time of these alleged incidents not even a resident of New York (or the United States). Accordingly, there is no internationally recognized justification for this kind of far-reaching exercise of extraterritorial jurisdiction. We further note that, as the Hon. Willem Geelhoed attests, if the situation were the reverse, the Netherlands would, as a matter of law and a policy to avoid diplomatic or political irritation from other countries, *refrain* from exercising extraterritorial jurisdiction under these circumstances (Ex. 10 ¶¶ 4-13, esp. ¶¶ 11-12). As a matter of comity and reciprocity, your Office should do the same. We discussed this issue with ADA Schott, but she expressed an unwillingness to change her position. Now that we have provided you with controlling legal authorities, we ask that you reconsider and stop prosecuting our client for any and all extraterritorial acts.

Cyrus R. Vance, Esq.
October 28, 2014
Page 14 of 17

V. It Appears that Your Office Was Misled Into Prosecuting this Case by a Series of False Statements and Fabricated Evidence.

A further reason to drop all charges against our client unconditionally are the very significant, indeed alarming, falsehoods that accompany Buiters's sworn statements to the police and your Office. This leaves your key witness without credibility at trial and casts serious doubt on our client's guilt.

The most troubling misleading information Buiters has provided concerns naked pictures of Mees masturbating, which Buiters told your Office that Mees sent him and which he claimed he experienced as annoying (Ex. 2 at 2). But apart from the fact that Buiters *requested* nude pictures from Mees (Ex. 6) (but was not given any), alarming new evidence we recently obtained from Buiters himself shows the opposite of what he represented to your Office: that Buiters *voluntarily* engaged in Skype sex with Mees of which he even took no less than 1,252 screenshots, which he then saved on his computer.¹¹ Mees never gave Buiters permission to record her and, in fact, told him not to. Both the fact that Buiters has been making extensive records of their Skype sex sessions and the fact that he was even on Skype clearly demonstrate that he lied when he claimed that Mees' nudity annoyed him. No one can be forced to go onto Skype and "undergo" the viewing of sexual activity.¹²

We stress that Mees takes this very intrusive invasion of her privacy very seriously and does not appreciate that their intimate love play has now apparently been shared with policemen, several people in your Office, and Buiters's three law firms. Buiters's actions may implicate Pen. L. § 250.45, which prohibits the surreptitious recording of a person's intimate parts without that person's permission. *See People v. Schreier*, 22 N.Y.3d 494 (2014).

Similarly troublesome is Buiters's evidence in support of his representation that "Mees caused him annoyance and alarm by sending him "over three thousand emails" (Ex. 3 at 2). This accusation appears to have been crucial to the ADA's decision to prosecute. Recently produced evidence shows, however, that this, too, was a lie. Buiters initially claimed that the 3,000 emails were sent "[b]etween November 9, 2009, and July 1, 2013" (*id.*). After Mees shared with your Office several emails showing that the relationship had *not* ended in November 2009 (*see* Exs. 14, 16-17, 19), Buiters changed his story. He now claims that 3,487 emails were sent "between July 12, 2012 and July 1, 2013" (Ex. 8 (Buiters Aff.) ¶ 4). The emails Buiters handed to your Office (which he produced to Mees only two weeks ago, as part of civil defamation case in the New York Supreme Court) show that 781 of them had gone straight into his spam folder, and thus could not have caused him any annoyance whatsoever.

¹¹ Buiters's actions may implicate Pen. L. § 250.45, which prohibits the surreptitious recording of a person's intimate parts without that person's permission. *See People v. Schreier*, 22 N.Y.3d 494 (2014).

¹² Buiters claims that Mees took the screenshots herself and emailed them to him, *and that they then accidentally and "automatically" got saved on his computer*. This is absurd. If it were true, Buiters should produce those emails or the screenshots in their native format, which will reveal on whose computer they were taken.

Cyrus R. Vance, Esq.
 October 28, 2014
 Page 15 of 17

Particularly alarming is that *no less than 536 emails are identical to other emails included in Buiter's batch*. In other words, in an apparent effort to ensure that even the post-July 2012 emails (as opposed to the post-November 2009 emails) added up to the 3,000 number, ***Buiter simply copied 536 emails multiple times***. (55 emails were printed as many as 10 times or more, and 21 emails more than 25 times; identical copies of the alleged "death wishes" were copied more than 11 times). Contrary to Buiter's representations, the total number of non-duplicative emails is not 3,487 but 1,397. Eliminating both the duplicates *and* emails from the spam folder that Buiter did not even see, the maximum number of emails Buiter could claim as "annoying," sent over the course of an entire year, is 616. Buiter's accusation inflated that number by a whopping 400%.

Disconcerting is further that while Buiter told your Office that Mees sent him 164 Facebook messages (Ex. 3 at 2), all evidence of those messages in their native format—necessary to determine their receipt extraterritorially—may recently have been destroyed, when on August 15, 2014, during the pendency of this case, *Buiter decided to close his Facebook account* (Ex. 26 at 2). We asked Ms. Schott if she has a copy of those Facebook messages but she has not responded. Both Facebook and Buiter have refused to unequivocally confirm that Buiter's action did not result in the destruction of highly relevant evidence.

Further evidence of significant falsehoods that misled your Office including the following:

- *Buiter represented that he has been telling Mees since November 7, 2009 to stop contacting him* (Ex. 3 at 2), as if he has been a victim of harassment and stalking ever since. It appears that the sheer length of Mees' purported intrusions into Buiter's life (several years) was an important factor in the decision to prosecute the case. But the statement was completely misleading because the sexual affair then continued, at Buiter's initiative, for at least another two-and-a-half years. Within a few months after his November 2009 message—but in any event no later than April 2010—Buiter had already changed his mind. On April 14, 2010, Buiter emailed Mees his hotel address in Amsterdam as soon as he arrived and asked for her plans for later that evening (Ex. 12). This flip-flopping characterized Buiter's attitude toward Mees throughout their relationship: presumably out of guilt or to maintain plausible deniability vis-à-vis his wife, he *tried* to say no; but he was never able to control himself for long. For example:

- On July 29, 2011, Buiter used harsh words when he told Mees she was "a stalker and harasser" and that "no more contact ever is the only solution" (Ex. 13). But *a few hours later* he agreed that Mees should show her "positive attributes" by showing her "hot pink suede dress" (*id.*).
- On August 9, 2011, Buiter again accused Mees of "stalking and harassment" (Ex. 14) but nevertheless told her they would not have Skype sex *for only "the next 3 or 4 days"* while his nephew and three friends were staying at his house (*id.*).
- On August 13, 2011, Buiter told Mees: "Just go away and stay away" (Ex. 15). But only a week later, on August 20, 2011, Buiter asked Mees if he could add her to his

Cyrus R. Vance, Esq.
October 28, 2014
Page 16 of 17

BlackBerry Messenger Contact list (Ex. 16), and a few hours after that he was driving over to Mees' apartment, as evidenced by his email asking for directions (Ex. 17).

- On June 22, 2012, Buitter told Mees "F... off and leave me alone forever" (Ex. 18). But only four days later, on June 26, 2012, Buitter reached out to Mees repeatedly on Skype late at night (Ex. 19). Eight days later, on July 4, 2012, Buitter began sexually provoking Mees by referring to himself in the midst of a business conversation as an "Enema-loving Brit" (Ex. 20).¹³

As this history of Buitter's communications indicates, even "serious" accusations of stalking meant nothing to Buitter, were pure window-dressing for his wife, and certainly did not mean that Mees "was previously *clearly* informed to cease" her conduct, as fourth-degree stalking requires. Pen. L. § 120.45(2) (emphasis added). Thus, when Buitter and his wife had their lawyer send Mees a cease-and-desist letter in February 2013, but Buitter repeatedly continued to try to contact Mees on Skype (Ex. 21), it was justifiable not to take that message seriously.

- *Buitter represented that Mees caused him annoyance and alarm by sending him sexually explicit messages (Ex. 3 at 2).* We believe that the ADA found this allegation troubling and an important reason to prosecute this case. But Buitter was not annoyed or alarmed by the use of sexually explicit language or by the receipt of such messages from Mees at all. In fact, at one point, after Mees sent him a sexually explicit message, Mees asked if he found her dirty now, to which Buitter replied "Why on earth would I?" (Ex. 23). The sampling of emails attached as Exs. 5 and 20 also leave no doubt that Buitter responded to Mees' messages with similar (or worse) sexually explicit language. They also show that Buitter himself *initiated* unsolicited sex talk (either initiating the conversation or responding to a business conversation with lewdness). The recently produced emails that Buitter gave your Office when he reported Mees shows that *none* of the vulgarity *he* sent to Mees was made part of the selection he chose to share with your Office. Buitter thus actively painted a one-sided picture of the relationship and misled your Office into thinking that sex talk is something that annoys him.

- *Buitter represented that Mees tried to meet him in his hotel in Beijing, China (Ex. 3 at 2).* An email we discovered after the ACD was entered shows, however, that this encounter was pre-arranged between Buitter and Mees. See Ex. 24 (for context, similar messages from Buitter advising Mees of his schedule so that they could meet up for sex are also attached).

- *Buitter represented that Mees harassed his children by sending them emails (Ex. 2 at 2).* It appears that, as one would expect, the special protection that the law accords to children was a very important factor for ADA Schott. But, as Ms. Schott will be able to confirm, there is actually not a single email from Mees to Buitter's "children" in the 3,000 pages of emails that Buitter gave her.

¹³ Buitter's inability to control his urges even continued after he had formally complained to the police about harassment and stalking in May 2013. On June 19, 20, 23, and 28, 2013, Buitter reconnected with Mees on Skype and tried to call her several times, including four days before her arrest (Ex. 21). After Mees was released from Riker's Island Correctional Facility, Buitter contacted her again (Ex. 22).

Cyrus R. Vance, Esq.
October 28, 2014
Page 17 of 17

- *Buiter further told your Office that he feared for the safety of his family (Ex. 3 at 2).* But this is nonsense. Not only did Mees never send the children any emails, Buiter's "children" are grown-ups in their twenties, who appear to live in California and Pennsylvania, far away from both Buiter and Mees. Each time he and his wife moved to a new apartment, Buiter made sure to advise Mees of the new address and contact information (*see Ex. 25*)—not something a real victim would do if he genuinely believed he was being stalked.

Accordingly, we respectfully suggest that the continued prosecution of our client has become unacceptable for multiple reasons that ought to lead your Office to do the right thing: to drop the charges and move the court to modify the ACD and dismiss this case unconditionally. We request an in-person meeting to discuss this matter further, and are available to answer any questions you may have.

Sincerely,

Ira D. London

London & Robin
99 Park Avenue, Suite 1600
New York, New York 10016

Counsel for Heleen Mees

Olav A. Haazen

Boies, Schiller & Flexner LLP
333 Main Street
Armonk, New York 10504

Counsel for Heleen Mees

EXHIBIT F



Grant & Eisenhofer P.A.

485 Lexington Avenue New York, NY 10017 Tel: 646-722-8500 Fax: 646-722-8501

Olav A. Haazen
Director
Tel: 347-841-8841
ohaazen@gelaw.com

123 Justison Street
Wilmington, DE 19801
Tel: 302-622-7000
Fax: 302-622-7100

1747 Pennsylvania Avenue, N.W., Suite 875
Washington, DC 20006
Tel: 202-386-9500
Fax: 202-386-9505

30 N. LaSalle Street
Chicago, IL 60602
Tel: 312-214-0000
Fax: 312-214-0001

May 9, 2016

Cyrus R. Vance, Jr., District Attorney
The New York County District Attorney's Office
One Hogan Place
New York, New York 10013

Re: *The People of the State of New York v. Heleen Mees*,
No. 2013NY050589 (N.Y.C. Crim. Ct.)

Dear Mr. Vance:

We write to follow up on our letter to you, dated October 28, 2014, and subsequent correspondence to Executive Assistant District Attorney Nitin Savur, and to request an independent investigation by a Special Victims Bureau member who has no prior involvement with this matter.

We represent Dr. Heleen Mees, a former New York University economics professor and consultant on Chinese affairs, who was briefly prosecuted by your Office for second-degree menacing, third- and fourth-degree stalking, second-degree harassment, and second-degree aggravated harassment. As we set forth in prior communications, our client's prosecution was based on a substantial number of false statements made by the accuser, Citigroup's chief economist, Willem Buiter, who falsely claimed to have fallen victim to harassment and stalking.¹ In March 2014, Mr. Savur agreed to end proceedings by way of an ACD, and on March 9, 2015, the case against Mees was dismissed.

We advised you in our October 28 letter that in the course of our civil damages case against Buiter, 1,251 photographs of our client were found on Mr. Buiter's laptop. As a result of that discovery, this matter has taken a different turn. The photographs show Mees' private parts and were taken without her knowledge or consent. The explanation Buiter provided for possessing these pornographic materials (which apparently were kept on his computer for years) was *not* that Mees had consented to these recordings but that *he did not take them* and that Mees had emailed him the pictures.² Mees categorically denies sending such emails.

¹ For a list of those falsehoods we refer to our October 28 letter.

² In fact, an accusation that Mees annoyed and alarmed Buiter by sending him nude pictures of herself was part of the criminal complaint Buiter filed against Mees on July 1, 2013.



Cyrus R. Vance, Jr., District Attorney
May 9, 2016
Page 2

Because Buiter was unable to produce the emails to which he claims the photos were attached³, we requested that your office start an investigation into a possible violation of Penal Law § 250.45 (surreptitious recording of private parts), which appears to have occurred during some of the many times Mees can prove she and Buiter had video cybersex via Skype. Mr. Savur and ADA Samantha Schott refused, however, on the grounds that (1) it could not be determined that Mees had *not* emailed them, and (2) Ms. Schott did not believe that the pictures were taken without Mees' consent (even though, as stated, Buiter specifically does not claim that he took them with Mees' consent). Mr. Savur added that we could contact the DA's Office and renew our request for an investigation if further evidence surfaced. We do so now.

The Forensic Investigation

After Buiter was ordered to turn over the photos in JPEG format as part of ongoing civil litigation, counsel for Mees commissioned forensic experts SBV Forensics to examine all 1,251 photographs and all forensically imaged computers that Mees has had in her possession since 2008. Based on this forensic analysis, SBV concludes that it is a near-certainty that Mees *did not take the photographs*, either with a phone, a standalone camera or a webcam, and that it is beyond a reasonable doubt that she *did not send the photographs* from any of her devices. SBV's report is attached for your convenience.

Specifically, SBV Forensic concludes with respect to the photo files:

1. Because the photos were produced in both PDF (1,388) and JPEG format (1,251), it can be determined through a comparison of MD5 hash values and "data carving" that Buiter in fact had more unique pornographic images of Mees in his possession than he represented (1,288 instead of 1,251). Among both the PDFs and the JPEGs there were also many duplicates (pp. 3-6).
2. Based on Mees' position in the photos, it is impossible that she manually took the photos herself. Because variations between successive pictures are mostly minor, which indicates only minimal intervals between them, it is also highly unlikely that the photos were taken in auto mode with a timer (pp. 6, 19-20).
3. The format of the photos (640 pixels by 480 pixels, for a total of some 300,000 pixels) is inconsistent with the use of a digital camera. Images taken with digital cameras are measured in *millions* of pixel ("megapixels") (pp. 7, 19).
4. The pictures' VGA resolution is, however, consistent with the use of either a webcam or a mobile phone camera (pp. 7-8, 19).

³ According to Buiter, the emails were deleted and only their attachments were saved, accidentally, as a result of his installation of a so-called "rule" in Microsoft Outlook, which automatically saves all attachments in a separate folder.

Cyrus R. Vance, Jr., District Attorney
May 9, 2016
Page 3

5. The low number of EXIF metadata captured on the JPEG files is inconsistent, however, with the photos having been taken with a mobile phone. It is also inconsistent with the use of a digital camera. Both would have registered additional metadata, such as various characteristics of the camera lens or the brand and type of the phone used (pp. 8, 19).
6. The EXIF metadata that was found, *e.g.* data indicating that no flash was used, excludes the possibility that the photos were stills derived from previously recorded video footage (which does not register any information on the use of a flash) (pp. 8, 19).
7. The depth and camera angles of the photos are also consistent with the use of a webcam (pp. 7, 19).
8. The picture files are consistent with screenshots taken during a live video chat on a platform like Skype. If the screenshots were taken on an Apple computer, however, such as used by Mees, Apple's operating system (Mac OS X) would have saved them as PNG files—not, as is the case here, as JPEGs (pp. 8-9, 19).
9. Photo Booth, which is a standard Apple application, does save photos in JPEG format but the photos' metadata is inconsistent with the use of this application because such use would have automatically registered "Photo Booth" as an IPTC field in each file (p. 9).
10. The photos have a resolution of 96 dpi, which is also not consistent with the use of Apple computers or digital cameras, which automatically generate images with resolutions of 72 dpi. The photos' 96 dpi resolution is, however, consistent with the use of a *Windows* computer (which Mees believes Buitter uses exclusively) (p. 10).
11. There is no indication on any of Mees' Apple computers that any metadata or file characteristics were manually manipulated. Manual editing would require opening, editing and re-saving each of the 1,288 unique picture files individually and would therefore be extremely time-consuming. No *Windows* programs and no virtualization software were found on any of Mees' laptops (pp. 10, 19).

With respect to Buitter's possession of the photos but not the emails by which they were supposedly transmitted, SBV Forensics concludes:

1. It is virtually certain that the photos were never on Mees' laptops. If they were, it would have been possible to retrieve or restore the files forensically. It is nearly impossible and technically very complex to individually remove files in a manner that guarantees the user that the files are forever irretrievable (pp. 11-15, 19-20).
2. No emails of the kind Buitter claims existed were found on Mees' computers. Secure removal of email files in a way that makes retrieval impossible also requires highly

Cyrus R. Vance, Jr., District Attorney
 May 9, 2016
 Page 4

specialized knowledge of the workings of the Mac OS X operating system⁴ (pp. 13-15, 20).

3. The “rule” that according to Buiter explains why the photos were saved, even though the emails purportedly attaching them were deleted, would have saved identical pictures only once, overwriting prior versions of the same attachment. The presence of duplicates of photos in Buiter’s files is therefore inconsistent with the workings of such a rule (pp. 17-18).
4. The rule is also inconsistent with the fact that a different picture (“moi.jpg”), which the parties agree *was* sent by Mees, was *not* saved in the same attachment folder, and that yet a third picture Mees sent (“plaatje.jpg”) was also not saved there⁵ (p. 18).

Accordingly, Buiter’s excuse for his possession of images of Mees’ private parts is not supported by forensics. This leaves no other reasonable explanation than that Buiter took the photos. The forensic investigation corroborates Mees’ account that their intimate interactions via Skype were never meant to be recorded, that she was unaware of the recordings, and that she never consented to being recorded.

We add three further observations. *First*, Buiter’s explanation that Mees sent him the photos implies that even he disagrees with Ms. Schott’s theory that he took them with Mees’ consent.

Second, according to Buiter, Buiter’s computer is now no longer available for forensic examination to determine if it was used to take the screenshots. The sole reason is that Buiter, as he has admitted in an affidavit, threw the computer away in December 2013. In other words, he destroyed the evidence *pending your Office’s criminal prosecution of Mees*, in which the alleged sending of annoying or alarming emails and nude photos was a significant issue for trial. If the original picture files had remained available, it would likely have been possible to compare their dates and times of creation with the parties’ erotic Skype sessions.

Third, Buiter disclosed in November 2015 that yet a third set of pictures exists, which was saved in PNG format in the cloud he has with U.S. internet provider Verizon. Your forensic examination of these files could shed light on the dates and method of their creation, and we respectfully request that you obtain these files for investigation. (While Buiter has produced PDF and JPEG copies of the photos to Mees, he continues to withhold the photos in PNG format).

⁴ In fact, SBV Forensics was able to restore a substantial number of emails (over 1,000) despite them having been previously deleted.

⁵ These two photos in JPEG format have characteristics different from the 1,288 files and *were* taken with a smartphone and Photo Booth, respectively.

Cyrus R. Vance, Jr., District Attorney
May 9, 2016
Page 5

Conclusion

We respectfully request that your Office commence an investigation and that this matter be assigned to a Special Victims Bureau member other than Ms. Schott, her direct supervisor Jeanine Launay, or Mr. Savur. When we previously requested an investigation, we found Ms. Schott defensive—even though we *never* accused the DA's Office of any errors—and she has been unwilling to even consider the possibility that she may have been bamboozled by an adulterer anxious to hide his affair from his wife and who had a sophisticated team of professionals behind him to convince the authorities of his accusations.⁶

The decisions to arrest and prosecute Dr. Mees have had profound consequences for Mees, who has lost her entire livelihood and is now an outcast in her business and academic circles. We find the ease with which Ms. Schott and Mr. Savur have brushed aside the severe collateral effects of an unjust prosecution to stand in stark contrast to the utmost protection they gave to a powerful adulterous Wall Street banker, who has four legal teams at his disposal and millions of dollars to combat a now-destitute 47-year old woman seeking justice. While we understand that it would be embarrassing, particularly for the Special Victims Bureau, if the DA were to conclude that it prosecuted the *victim* of a felony sex crime and protected the man who may have been the perpetrator, that does not justify such defensiveness or failure to take a victim's story seriously. Mr. Savur and Ms. Schott know, of course, that a victim does not have the burden of proving that she did not consent. It was improper for them to demand that Mees prove that she was genuinely sexually violated. We ask that you assign an independent investigator to investigate if Penal L. 250.45 was violated and if so, by whom.

We request an in-person meeting with you to discuss this matter further, and remain at your disposal if you have any questions. Please do not hesitate to contact me at (347) 841-8841 or ohaazen@gelaw.com, or Brooke Alexander at (914) 749-8231 or balexander@bsflp.com.

Sincerely,



Olav A. Haazen

⁶ In the civil case, Buiter has tried to distance himself from the false July 1, 2013 police report by arguing that those were not his own words. The evidence in that case shows that Buiter hired a criminal lawyer and two ex-NYPD officers who acted as in-betweens and were in constant contact with Buiter and the NYPD up until the exact minute that Detective Roadarmel signed the July 1 report.



Report for
Houthoff Buruma Coöperatief U.A. in Rotterdam

Regarding
Examination of Pictures - H. Mees



FOREWORD

Dear user of this report,

SBV Forensics B.V. (hereinafter SBV Forensics) is specialised in (internal and external) prevention, examination and/or remedying of irregularities, illegalities and/or punishable acts and therefore aims to establish the truth.

The objective or absolute truth does not de facto exist. However, the examination carried out by SBV Forensics can provide a basis for conclusions that reflect the most probable truth. The highest degree of certainty that can be provided by an expert with respect to facts reconstructed after the event is 'with a probability bordering on certainty', also referred to as 'incontrovertible'. The lower limit lies at 'with a probability bordering on certainty'. And in between there are a number of varying degrees of (im-)probability. On a scale this is reflected as follows:

Probability	Qualification
100 %	With a probability bordering on certainty
90 %	Most likely
75 %	More than likely
50 %	Likely
0 %	Denial of any opinion
-/- 50 %	Unlikely
-/- 75 %	More than unlikely
-/- 90 %	Most unlikely
-/- 100%	With an improbability bordering on certainty

This report is a 'work' within the meaning of article 10 of the Dutch Copyright Act 1912 and is usually provided 'strictly confidential' to the commissioning party. The copyright to this work is vested in SBV Forensics. Dissemination or use hereof without the prior approval of SBV Forensics is, other than in the cases by or pursuant to the law or case law, therefore not permitted (article 31 et seq. Copyright Act 1912). The ban on dissemination and use also applies to the successive acquirers.

SBV Forensics



SBV
Forensics

Report on
Examination of Images - H. Mees

TABLE OF CONTENTS		Page
1	Introduction.....	1
2	Assignment.....	1
3	Source data.....	1
3.1	Hard disks.....	1
3.2	Pictures	2
3.3	E-mail messages with picture	3
3.4	Affidavit and Exhibit 9	3
4	Creation of Pictures	3
4.1	Introduction	3
4.2	Findings.....	3
4.3	Evaluation.....	10
5	Presence of files on hard disks.....	10
5.1	Introduction	10
5.2	Presence of files.....	11
5.3	Deleted files	12
5.4	Secure erasure of files	13
5.5	Evaluation.....	15
6	Email messages 'me myself and I'	15
7	Email messages 'I miss you'	16
8	Rule for storing attachments	16
8.1	Introduction	16
8.2	The way the 'rule' works	17
8.3	Ratio for the use of the 'rule'	18
8.4	Evaluation.....	18
9	Concluding remarks	19



1 Introduction

In proceedings between Mrs H. Mees (hereinafter referred to in short as: the Client) and Mr W.H. Buiter and Mrs A. Sibert Buiter (hereinafter jointly referred to in short as: the counterparty or separately as: Buiter or Sibert) questions arose regarding the creation and origin of approximately 1,250 images on a USB stick sent to us by Houthoff Buruma (hereinafter the Pictures). We were informed that this USB stick is a copy of a USB stick provided by Buiter to the Client's lawyers.

With a view to answering these questions, the Client's Dutch lawyer, professor Mr. M.E. Koppenol-Laforce, instructed SBV Forensics on behalf of the Client to examine the properties of these Pictures. Furthermore, with a view to being able to form an opinion with regard to the source of these Pictures, SBV Forensics was also provided with three so-called images of hard disks of (laptop) computers belonging to the Client.

2 Assignment

Having regard to the above, the following assignment was agreed upon:

"SBV Forensics will examine the properties of the Pictures with a view to establishing the most probable method of creation. SBV Forensics will also examine three images of hard disks of (laptop) computers belonging to the Client with a view to establishing whether the relevant Pictures were created with one of the computers she used, or whether these Pictures were found on one of these computers, and whether these Pictures were sent from one of these computers to Mr Buiter.

In addition, SBV Forensics will examine a picture created by the Client as sent by her by email to Mr Buiter, and compare this with the Pictures."

On performing the activities we discovered another picture¹ created by the Client and sent by her to Mr Buiter. As requested by the Client's Dutch lawyer, we also examined this picture and compared it with the other Pictures.

The Client's Dutch lawyer has informed us that Buiter has declared that he installed a small 'program' which ensured that attachments to email messages were saved separately to a specifically designated location. The Client's Dutch lawyer has instructed us to assess the use of the 'program'.

3 Source data

3.1 Hard disks

SBV received an external hard disk from the Commissioning Party which contained three so-called images.

An image (created in a forensically sound manner) is a bit-by-bit duplicate of a data carrier that, accordingly, is completely identical to the source data carrier. Through the

¹ The Dutch version of this report uses the word 'afbeelding', which translates to 'image'. To avoid confusion with the technical term 'image' used to describe a copy of a data carrier, throughout this report, the word picture is used to describe a (digital file containing a) (photo)graphic depiction.



forensically sound creation and processing of an image, digital forensic examination can be carried out without any risk that the digital evidence will be lost or altered.

The images received by us were stated to be created of three (laptop) computers used by the Client. The images received can be described as follows:

"MacBook"

Brand hard disk	:	Toshiba MK6034GSX
Serial number	:	Z6EIT1ZJT
Capacity	:	55.8 GB (60.011.642.880 Bytes)
Image created on	:	30-04-2015
SHA hash	:	d95f566eb67b44c60ab6675a7125598f69- aae920a26f70f928410690abd41574

"MacBook Pro"

Brand hard disk	:	Fujitsu MHV2120BHPL
Serial number	:	NW81T6825U59
Capacity	:	111.7 GB (120.034.123.776 Bytes)
Image created on	:	27-02-2015
MD5 hash	:	8F4C46823F9B913636B6504C258FD4BE

"MacBook Primary"

Brand hard disk	:	Hitachi HTS545025B9SA02
Serial number	:	100726PBL200CSHAH90N
Capacity	:	232.8 GB (250.059.350.016 Bytes)
Image created on	:	27-02-2015
MD5 hash	:	8F248A43122AB50C5AC7EB8C0E0F8BCF

Based on the data found, we consider it most likely that the images have been created in a forensically sound manner. To examine the images we received we processed them with Forensic Tool Kit version 5 of Access Data.

It is clear to us from the examination of the images that there is no partition on any of the above-mentioned computers on which the Windows operating system is or can be installed. Neither do the above-mentioned computers contain virtualization software by means of which the Windows operating system can be used in a 'virtual machine'.

3.2 Pictures

For the purpose of our examination we also received a USB stick containing 1,250 Pictures in JPEG format (.jpg), among others. According to the file properties these Pictures were last modified on 15 December 2013.



3.3 E-mail messages with picture

The Client's Dutch lawyer informed us that the Client sent several email messages to Buiter in mid 2011. The subject of these messages was always 'me myself and I'. These messages included an attachment with a file with the name 'moi.jpg.' This relates to a picture that the Client acknowledges to have created herself.

The Client's Dutch lawyer has provided us with these email messages for the purpose of our examination. Our findings in relation to this picture are included in chapter 6.

3.4 Affidavit and Exhibit 9

The Client's Dutch lawyer has informed us that Buiter declared in an Affidavit dated 11 August 2015 that he installed a small program which ensured that attachments to email messages were saved separately to a specifically designated location. An example of such a program was allegedly attached to the Affidavit as Exhibit 9.

The Client's Dutch lawyer has provided us with a copy of the Affidavit and Exhibit 9. Our finding with regard to the use of this 'program', as described in aforementioned documents, are included in chapter 8.

4 Creation of Pictures

4.1 Introduction

As stated in paragraph 3.2 we received the Pictures for analysis. The file names comprise sequential numbers placed between brackets, followed by the extension .jpg.

The file names run from (1).jpg up to and including (1387).jpg. Various intervening numbers are missing. We do not know whether the missing numbers exist or existed.

This chapter contains the findings of our analysis of the Pictures, with a view to being able to determine the most probable method of creation.

4.2 Findings

Numbers of pictures

As also stated in paragraph 3.2 we received a USB stick containing 1,250 Pictures in JPEG format.

A so-called hash value can be calculated using a complicated algorithm for each digital file. For this purpose various algorithms are used of which the most common are MD5, SHA1 and SHA256.

The chance that different files will have the same hash value is extremely small (whereby it holds that the more complicated the algorithm, the longer the hash value and the smaller the chance). A hash value can therefore be regarded as a digital fingerprint or the digital DNA of a file: the file is identified by the hash value.



In this respect it must be pointed out that it concerns the file content. Two files with different names and different file extensions (for example, Photo1.jpg and Picture2.gif) will have the same hash value if they have the same content. The reason being that the file name is not embedded in the file but is recorded by the file system.

We determined the MD5 hash value for the 1,250 Pictures to be analysed. By comparing these MD5 hash values, we established that 33 photos appeared 2 or 3 times (in total 88 files). Accordingly, we received 1,195 unique pictures.

The USB stick contains not only the Pictures, but also a PDF file called 'Mees Pictures.pdf'. This file comprises 1,388 pages, with one photo on each page.

The type (picture, text etc.) of a specific file can be established on the basis of unique codes at the beginning and at the end of the file.² A data carrier can be examined using specific software, such as the investigation software we use, on the basis of the code that refers to the beginning of a file of a certain type (for example a JPEG file) and to a corresponding code for the end of a file of that type. Both codes and the intervening data will therefore be considered and interpreted as a file of that type. This process is known as 'data carving'. Data carving can, however, also be applied to a file so that embedded elements such as pictures, can be identified.

The investigation software used by us could, through data carving in the 'Mees Pictures.pdf' file, identify 1,282 JPEG pictures. By comparing the MD5 hash values, we determined that these did not contain any duplicates. The 'Mees Pictures.pdf' file therefore contains at least 1,282 unique pictures. (The result of data carving is determined by the condition of the source material on the one hand, and the software used for data carving on the other hand. It is therefore possible that there are more embedded pictures in the file than found by the software. For that reason reference is made to 'at least' the number of files mentioned.)

Four PDF files 'Exhibit L Photographs Mees Sent Buiter [number sequence].pdf' were sent to the Client's lawyer by the counterparty.³ These four files contain 1,252 pages, with one picture on each page. The first page contains picture that has a strong visual likeness to the picture 'moi.jpg' as sent by The Client to Buiter by email (see also chapter 6). This picture, or at any rate a picture with a strong visual likeness thereto, is not on the USB stick and also does not appear in the earlier 'Mees Pictures.pdf' referred to. The investigation software used by us could, through data carving in this file, identify 1,196 JPEG pictures. By comparing the MD5 hash values, we determined that 9 pictures appeared twice. The four PDF files of Exhibit L accordingly contain at least 1,187 unique pictures.

² The file name and the extension attached thereto (for example, Textfile.doc) are not part of the file, but are registered by the file system. If the name of the example file is changed to Textfile.jpg, it can still be identified as a file that can be opened by means of a word processor on the basis of these codes.

³ The Client's Dutch lawyer has informed us that the Exhibit L files ('Exhibit L Photographs Mees Sent Buiter 1-300.pdf', 'Exhibit L Photographs Mees Sent Buiter 301-600.pdf', 'Exhibit L Photographs Mees Sent Buiter 601-900.pdf' and 'Exhibit L Photographs Mees Sent Buiter 901-1252.pdf') were sent by Buiter's American lawyer to the Client's American lawyer on 10 October 2014. The Client received these files from her lawyer on 13 October 2014 by email.



We have summarised the above-mentioned findings in the following table:

	USB stick (1,250 JPEG files)	USB stick (‘Mees Pictures.pdf’)	Exhibit L (PDF files)
Number of files	1,250	1	4
Number of pictures	1,250	1,388	1,252
Identified on the basis of data carving	Not applicable	1,282	1,196
Duplicate pictures on the basis of files	33	Not applicable	Not applicable
Duplicate pictures on the basis of data carving	Not applicable	0	9
Number of unique pictures	1,195	$\geq 1,282$	$\geq 1,187$

Table 1 – Summary overview numbers of pictures

From the above it follows that it is not clear which files the Client allegedly sent to Buiter by email. In this chapter we restrict ourselves to the 1,250 Pictures (comprising as already stated 1,195 unique pictures).

File names

Devices for recording digital images use a convention for the naming of the resulting files. A digital camera customarily uses the code DSC (an abbreviation for Digital Stills Camera) followed by a sequential number or a combination of date and sequential number.

When using the functions of the operating system of a computer (for example, the function to create a screen image) or specific applications, the software determines which naming convention is used. In addition, the moment when the image is created is usually included in the file name.

Nevertheless, there are also applications that use a naming convention with only a sequential number or a combination of a descriptive element (for example, 'picture') followed by a sequential number. Furthermore, there are two variants in practice.

The first variant relates to the application where each time that it is started up and used, again begins with the lowest number. The second variant relates to the application that uses a number that directly follows the highest number found. This second variant is not common in practice and then, in particular, in relation to applications that always save files to a default file location.

As will be set out in more detail below, it can be concluded from the picture content that the Pictures were created in a couple of separate sessions.

Taking into consideration that the file name contains only a sequential number as well as the fact that numbering did not restart at the first Picture from a new session, we deem it most unlikely that the Pictures were initially captured with the file names as used on the USB stick.



This implies that it is most likely that the file names were changed later on into (only) a sequential number placed between brackets. The large number of files makes it most unlikely that the file names were changed manually, accordingly it is most likely that a specific tool or specific functionality of the operating system of the computer was used. Given that an uninterrupted number sequence is used on automated execution of this type of task, we accordingly deem it most likely that also the currently missing numbers were attributed to (picture) files in the aforementioned process.

In combination with the findings from table 1, this justifies the conclusion that the USB stick does not contain all Pictures that exist or existed.

Composition and picture content

The Pictures were created in a few separate sequences, each sequence comprising various pictures with the same, fixed background: a fixed camera position was used. In addition the position of the Client, as appearing on the Pictures, furthermore shows a relatively minor movement.

Besides, given the position of the Client she was not able to operate the recording device. It is explained below why a function to delay the recording moment ('self-timer') was not used.

The sharpness of the Pictures is, in particular, as a consequence of the 'image noise', quite low. Nevertheless, it seems as if there was a relatively large 'depth of field': in other words, that both subjects close to the lens as well as subjects further away from the lens are sharply recorded. This points to the use of a lens with a short focal length. Because the photos show no strong perspective deviation of parts that are close to the camera, it follows from the focal length used that a normal field of view or moderate wide-angle was used.⁴ A normal field of view or moderate wide-angle with a short focal length indicates a small image sensor.

The Pictures show a large quantity of 'noise'. On the one hand this also suggests a small image sensor and on the other hand it indicates little light as is usually the case indoors. It can be concluded from the absence of strong shadows that no additional light sources, such as a flash or a permanent (auxiliary) lamp, were used to compensate for the limited light quantity.

On the basis of the compositions and picture content, we deem it most likely that the images belonging to one series were made briefly after one another. The short time between successive images suggests that no 'self timer' was used. Therefore it is most likely that the Pictures were not realized through actions of the Client on or briefly before the moment of the recording.⁵ The Pictures were most likely made with the use of a recording device with a lens with a short focal length and a small image sensor, without the use of auxiliary lighting.

⁴ A normal field of view is understood to mean one that, in terms of perspective, corresponds with that of the human eye. A lens with a wider field of view is referred to as a 'wide-angle lens', a smaller field of view as a 'tele photo lens'. A wide-angle lens relatively enlarges subjects that are close to the lens as a result of which the natural proportions are distorted. For a full screen portrait photo made with a (ultra) wide-angle lens it is characteristic that the nose of the portrayed person is shown as much too big. Conversely, a (long) telephoto lens has a compressive effect.

⁵ Below we separately discuss the possibility of recording a video from which stills are separately stored as pictures afterwards.

*File format and picture size*

The Pictures are all in the file format JPEG. This is a generally customary, compressed file format for pictures (similar to the MP3 format for audio files), in which the compression is applied to reduce the file size at the expense of some image quality.

The files are mainly in the format 640 pixels wide and 480 pixels high. Therefore there is a 4:3 aspect ratio (ratio between width and height). This format is also referred to as 'VGA resolution'. A limited number of images, 69, has a 4:3 aspect ratio, but is smaller in size: 320 x 240 pixels.

Digital single-lens reflex cameras or system cameras, with some exceptions (this particularly concerns the cameras with a so-called Four Thirds or Micro Four Thirds sensor as well as some systems for professional use) have an aspect ratio of 3:2.

The aspect ratio 4:3 is particularly used as (standard) aspect ratio by compact cameras, mobile phones, video cameras that do not support HD format and webcams such as those built-in or connected to computers.

The picture size 640 x 480 pixels, in total therefore over 300,000 pixels, is much more limited than the number of pixels of a photo made with a compact camera: with compact cameras, the picture size is shown in millions of pixels ('megapixels'). The VGA resolution has also for a long time been the standard for the cameras of mobile phones and webcams. Such cameras have a small sensor and use a lens with a short focal length.

The picture size and the aspect ratio of the Pictures (VGA resolution) as well as the picture content (in particular the large quantity of noise and the large depth of field, which are both indicators for a small image sensor) and the fixed camera position are in accordance with the use of a webcam (connected to a computer or built-in to a computer) or a mobile phone (also see below).

Meta data

Meta data is added to digital files on several levels. This occurs for instance on the level of the file system, the part of a computer system that is responsible for the systematic writing, reading and deleting of files: for instance, the file system registers when a file was made, when it was last modified etc.

The so-called EXIF standard has been developed to add meta data to picture files. Devices that support this standard can add meta data to (certain types of) files in which the picture created by the device is recorded.

A compact camera that records a photo as a JPEG file can include EXIF data in that file, such as the focal length of the lens, the diaphragm settings, the used shutter speed etc. What information is added to a picture file as EXIF data is determined by the developer of the recording device.

We established that only very limited EXIF data is present in the provided files. More specifically this concerned: a resolution of '96 dpi', flash mode 'no flash', ISO value '0', exposure mode 'Unknown' and white balance 'Automatic'.



The limited EXIF data is an additional indicator that the Pictures were not made with a digital camera.

Also when using the camera of a mobile phone, more EXIF data is added to the JPEG picture file, such as for instance the make and type of the telephone (for an example also see chapter 6). The absence of these details is a strong indicator that no mobile phone was used to make the pictures.

Video

Before 'HD Ready' and 'Full HD' (an aspect ratio of 16:9 and an image size of 1,280 x 720 pixels, respectively 1.920 x 1.080 pixels) were generally marketed, digital video cameras (or the video functions of compact cameras and mobile phones) used what is retrospectively called 'SD' (standard definition, the image size also known as VGA resolution of 640 x 480 pixels in an aspect ratio of 4:3).

It is therefore conceivable that the Pictures were made through the production of a video file, from which stills were saved as separate Pictures afterwards with software.

EXIF data is also added to video recordings.⁶ However, this data is very limited. Various EXIF data found in the Pictures, such as regarding the use of a flash, are usually not recorded in video recordings. Therefore we deem it most unlikely that the Pictures were made by saving separate images from a video recording.

Use of a webcam

On the basis of the above we deem it most likely that the Pictures were made with the use of a webcam. There are nevertheless various manners in which the picture of a webcam can be recorded into a file.

The first and most obvious method is the use of functions used for that purpose in the software with which the webcam is controlled. There are various applications that use a webcam. This particularly concerns applications that are focused on the realization of a remote picture connection. The best known examples hereof are applications for video phone calls / video chats, such as the platform independent Skype application or the program limited to the Apple platform called Facetime.

Many of such programs offer the possibility to record the picture of the webcam (a video stream) during a session. Initially only as a (still) picture later on also sometimes as a video.

As the counsel of Client, professor Koppenol-Laforce informed us, the Client was regularly in touch with Buiters.⁷ A Skype application offers the possibility to record the picture of the webcam of the session partner during a Skype session. This function was initially called 'Video Snapshot', but in later versions of the application it is called 'Take Picture'.

⁶ The EXIF standard was developed for still images. However, upon opening video files in an image editing program EXIF data is shown.

⁷ In our investigation of the images made available to us, we established that Skype was installed onto all three computers of the Client. On all three images (of the hard disks of the computers) we found files in which the history of Skype sessions is recorded through the Skype application.



In the versions of the Skype application developed for the Apple platform, however, the 'Video Snapshot' or 'Take Picture' function is missing. This is because the operating systems for Apple computers, Mac OSX, elaborate functions are already built-in to record pictures. The 'screen shots' recorded by Mac OSX are stored in the PNG format instead of the JPEG format.

Apple computers are always provided with an application with which photos can be taken with the aid of the webcam of the computer. This application does store the images in the JPEG format, but in the process records the name of this application, Photo Booth, as a IPTC field.⁸ However, this information is not included in the meta data of the Pictures made available for analysis.

Applications in which webcams are used for the realization of video connections, usually offer the possibility to make two video streams visible on screen: the picture that is recorded through the webcam of the session partner, but also the picture of the own webcam (often shown as 'picture in picture'), so that the computer user can for instance easily check if he or she is 'fully on camera'. In order to avoid coordination problems with the computer user, the picture of one's own webcam is shown in mirror image. If this image is recorded in the form of a screen shot, this therefore results in a mirror image. This is also the case when using the Photo Booth application mentioned above with its standard settings.

Research on the internet pointed out that various versions of Skype for Windows allegedly had the possibility to mirror the image of the webcam horizontally, so that a correct picture can still be presented. We did not find indications that such a setting is also present in Skype versions for Mac OSX, however, we have not carried out elaborate investigations into this matter.

As the Dutch counsel of the Client informed us, the Client in any case had Skype sessions with video connection with Buiter in the period around 2009-2012.⁹ In this period various laptop computers of Apple already had a built-in webcam with a resolution of 1,280 x 1,024 pixels. For the control of this webcam, software developers could use the so-called APIs developed by Apple. However, these only supported a 640 x 480 resolution ('high quality video') or 320 x 240 ('standard quality video'). This clarifies why the Skype partners of an Apple user with a high resolution webcam (at that time) still only received pictures in a lower resolution.¹⁰

Picture resolution

The picture resolution can also be stored in the EXIF data of a picture file. This term is in a way confusing because for the term of the picture size (the total number of pixels that form a picture) the term resolution is also often used.

⁸ IPTC is a standard for meta data that can be added to pictures. Where EXIF data is focused on and follows from the (settings on the) device with which the pictures were made, IPTC is mainly focused on the picture content. In this way, keywords can for instance be recorded which provide a description of the content of the picture ('house', 'tree', 'sunset') or the contact details and copyright notice of the photographer. IPTC data must usually be added by the user afterwards. The automatic addition of an IPTC label 'Photo booth' is therefore atypical.

⁹ On the images of the computers of the Client, we found various databases in which the Skype application stores the history of Skype sessions. In these databases we established that during various Skype sessions a registration number of a picture recording device was registered. These numbers most likely refer to the built-in webcams of the computers of the Client. Because for our investigation we exclusively had the disposal of the images as mentioned in chapter 3, and not the computers, we have not been able to verify this.

¹⁰ See for instance <https://discussions.apple.com/thread/2293095?tstart=0>.



Picture resolution is the number of pixels that is shown per unit of the output device. The picture resolution is stated in dots per inch (dpi).¹¹

While in an Apple environment and also in respect of the majority of the digital cameras a default resolution of 72 dpi is given to pictures,¹² the default resolution that is used by Windows for pictures is 96 dpi.

As indicated above, the resolution of the Pictures is 96 dpi according to the EXIF data. This is a strong indicator that the Pictures were recorded within a Windows environment.

Adjustment of files

It cannot be ruled out that the Pictures were initially created in another picture form (moving images instead of stills) with another picture size and/or another file format and were changed afterwards. Editing picture form, picture size, picture resolution and file format is after all possible with nearly every video application and/or image editing application. It is also very easy to edit file properties and/or EXIF data with various simple tools which can for instance be found on the internet.

If the Pictures were manipulated with the aid of the applications on the computers of the Client, the end result (the 1,250 Pictures, either or not in an edited form) should at some time also have been stored on the computers of the Client. However, as will be set out in greater detail in chapter 5, we have not found indicators of this.

4.3 Evaluation

Given, inter alia, the file size, the camera position, the depth of field and the meta data, we consider it most likely that the Pictures that were submitted for analysis were originally created using a webcam. Furthermore, given the picture resolution we consider it most likely that the initial storage of these pictures took place in a Windows environment.

As pointed out in chapter 3, we did not find a Windows environment or virtualization software on the images. Therefore, we consider it most unlikely that the Pictures were initially stored on one of the Apple computers used by the Client.

5 Presence of files on hard disks

5.1 Introduction

We pointed out in chapter 4 of this report that the Pictures were most likely originally created by using a webcam and were initially stored in a Windows environment.

¹¹ Use of this standard unit is not undisputed or at least not always equally accurate. Dependent of the type of output device (old TV screen, modern LCD screen, ink jet printer, raster image processor etc.) sometimes the term ppi (pixels per inch) or lpi (lines per inch) more suitable. In practice usually dpi is simply referred to.

¹² Apple's own application Photo Booth is a remarkable deviation: dependent of the version and the computer on which it has been installed, the picture resolution is sometimes registered and sometimes not registered in the EXIF data. On a modern iMac operating with Mac OS 10.10, Photo Booth registers a picture resolution of 72 dpi in the EXIF data. The picture discussed in chapter 7 which was found on the image of the 'Macbook Pro' does not contain any picture resolution in the EXIF data.



Even though we consider this most unlikely, it cannot be fully excluded that the Pictures were created with a recording device linked to a computer of the Client, whether or not operated by a third party.

For example, in theory, it is possible that a screen shot was made of the mirrored webcam picture and the specific picture was subsequently edited in an image editing program and flipped horizontally in doing so, after which the EXIF data of the file were adjusted, by means of a specialised tool, to the values we found in the files. However, performing this picture editing manually is very time consuming.¹³

Likewise, it is possible in theory that a video file was created, of which individual pictures were saved as separate files, after which the EXIF data were also adjusted by means of a specialised tool. However, the process of manually creating a still picture from a video file is very time consuming.¹⁴

Furthermore, the Dutch lawyer of the Client informed us that the other party asserts that the Client sent the Pictures by email.

In order to examine whether these options may have occurred, we examined the images of the hard disks from the computers of the Client for relevant digital evidence.

5.2 Presence of files

The three images contain a total of 871,147 graphic files. In total, 430.615 of these files are in JPEG format.

It is infeasible in the course of a brief examination to assess the contents (in other words: visually) of such a large number of files. For this reason, we therefore used a different method to establish whether the files containing the Pictures are on the images.

As is also explained in paragraph 4.2, a so-called hash value can be calculated using a complicated algorithm for each digital file. For this purpose various algorithms are used of which the most common ones are MD5, SHA1 and SHA256.

The chance that different files will have the same hash value is extremely small (whereby it holds that the more complicated the algorithm, the longer the hash value and the smaller the chance). A hash value can therefore be regarded as a digital fingerprint or the digital DNA of a file: the file is identified by the hash value.

In this respect it must be pointed out that it concerns the file content. Two files with different names and different file extensions (for example, Photo1.jpg and Picture2.gif)

¹³ Manually editing the Pictures in the manner stated above requires the pictures to be opened, edited and saved again in several applications (both an image editing program and an EXIF tool). Therefore, this is a very time-consuming process. Several applications for editing pictures have the option to process multiple pictures at the same time (batch processing) or to apply multiple successive edits on multiple files (such as performing 'actions' in Photoshop). The use of batch processing or similar techniques requires more than average knowledge of the specific software. Furthermore, it must be considered that the files are stored in the JPEG format. As indicated earlier, this is a compressed format. If these files are edited and saved again, the file compression will cause the picture quality to deteriorate more and more. Whether the picture quality deteriorates as a result of repeated compression is difficult to establish and we have not examined it either.

¹⁴ Because the moment on which the still picture is extracted must be selected by the user, this step will most likely always be performed manually. For the subsequent editing of these pictures, the same findings apply as indicated in the previous footnote.



will have the same hash value if they have the same content. The reason being that the file name is not embedded in the file but is recorded by the file system.

We determined the MD5 hash values for the 1,250 Pictures to be analysed. Subsequently, we also calculated the MD5 hash values for all 871,147 graphic files on the images.

If the aforementioned 871,147 graphic files also contain one or more of the 1,250 Pictures, whether or not with a modified file name, then the MD5 hash values must be identical. However, we established that there are no identical hash values. Therefore, it can be concluded with a probability bordering on certainty that none of the 1,250 Pictures were found on the images of the Client's computers.

5.3 Deleted files

If a file is deleted by a user, it is not physically deleted from the data carrier. Only the reference to the location on which the file is saved on the data carrier is removed by the file system. The relevant storage space on the data carrier is released by the file system, so that other files can be saved on that same location. In due course of time, a file that has been "removed" by a user will be physically overwritten.

By physically reading out a data carrier bit by bit, removed files can be recovered at a later time, at least as long as they have not been overwritten by other files.

With the help of the FTK program we used for this investigation, we also examined the images for deleted files. Simply put, in doing so, the software searches for the code that alludes to the beginning of a file of a certain type (for example, a JPEG file) and to the corresponding code for the end of a file of that type. Both codes and the intervening data will therefore be considered and interpreted as a file of that type. This process is known as 'data carving'.

The files recovered as a result of data carving were also included in the analysis of MD5 hash values that was described in the previous paragraph. Therefore, it can be concluded with a probability bordering on certainty that none of the 1,250 Pictures have been stored on the Client's computer, were later deleted and could still be fully recovered.

However, if the intermediate data has been partially overwritten, or corrupted, the file content will no longer be identical to that of the original file. In that case, comparing the MD5 hash value cannot give a definite answer on whether one or more of the 1,250 Pictures have been stored on the Client's computer, were later deleted but could not be fully recovered.

Only a visual assessment can give a definite answer in this respect. In the free disk space (i.e., the disk space that, according to the file system, is available to store new files) a large number of JPEG files which have been fully or partially recovered through data carving are located on the images, which files we have visually assessed for similarities with the 1,250 Pictures.

On the hard disk of the MacBook, this is a total of 22,808 JPEG files. These files do not contain any files that show a visual resemblance to one or more of the 1,250 Pictures.



On the MacBook Pro and the MacBook Primary, there are 23,981 and 171,923, respectively, fully or partially recovered JPEG files in the free disk space. These files include a large number of files that show a visual resemblance to one or more of the 1,250 Pictures.

Further analysis of the images showed that these Pictures were included in deleted PDF files, which could still be fully recovered through data carving. By comparing the MD5 hash values of these deleted PDF files with the MD5 hash values of PDF files that had not been deleted yet, we could establish that these concerned deleted copies of the files "Exhibit L Photographs Mees Sent Buiter [number sequence].pdf" (i.e. the PDF files the Client received from her lawyer).

That these files were not found when comparing the MD5 hash values as described in the preceding paragraph is not the result of the partial overwriting or corruption of these files.

On the one hand, the differences between the MD5 hash values are the result of the fact that when compiling the PDF files, only the content of the pictures has been enclosed for Exhibit L (in other words: the EXIF data is lacking in these pictures) and on the other hand, the fact that the Pictures were included in the PDF in a smaller format: the majority of the Pictures was reduced in size from 640 x 480 pixels to (for example) 160 x 120 pixels.

5.4 Secure erasure of files

Files that have been deleted by a user, as explained above, can be recovered as long as the relevant disk space is not overwritten by other files.

However, users can also "securely erase" files. This means that the disk space used by the file that is to be deleted is immediately overwritten with meaningless information.

For this purpose, special tools can be used that overwrite files and/or folders or the entire disk space that is considered freely available by the file system in its entirety with meaningless information.¹⁵

The operating system for Apple, Mac OS X, was standard already provided with two different options to securely erase files: the Finder, the program to manage and navigate through files and folders, similar to the Windows Explorer program in Windows operating systems, contained the option to securely empty the "Trash". If this option was chosen, the disk space of the files the user transferred to the "Trash" was immediately overwritten with meaningless information.

A second option was included in the tool "Disk Utility" which provided the option to overwrite the full free disk space with meaningless information.

The use of a tool to overwrite the full free disk space can be noticed in a relatively simple manner in the examination of a data carrier. If in an intensively used computer most of the free disk space merely consists of the value 0 or 1 or a repeating pattern thereof and hardly any deleted files can be recovered through data carving, it is more than likely that such a tool has been used.

¹⁵ Depending on the tool, the disk space is overwritten one or several times with 0 or 1 on bit level or a random pattern thereof. With various tools, the user can choose the manner in which the overwriting takes place.



Given the large number of files found on the images, the computers of the Client were most likely used intensively. Given the large number of files that could be "recovered" through data carving, we consider it most unlikely that a general tool to overwrite free disk space has been used on these computers.

It does remain theoretically possible that individual files have been removed securely in a way that can be demonstrated hardly or not at all: if individual files are securely erased, as is the case when securely emptying the 'Trash', only small amounts of disk space are overwritten. The use of such a method can be demonstrated hardly or not at all by examining the free disk space. Therefore, it remains theoretically possible that one or more of the 1,250 Pictures (in original size) were once stored on the hard disks of the Client's computers, but that the Client deleted these Pictures in a secure and irrecoverable manner.

This comes with two comments that most likely preclude the application of such a process by the Client.

In the first place, it must be pointed out that secure erasure in the manners described above does not guarantee that the information cannot be recovered. After all, the recent versions of Mac OS X (from Mac OS X 10.6) provide the option for programs to save files automatically. This way, users can never lose any information because they forget to save their work. In order to make this possible, copies of files are stored by the operating system. However, these copies are not always stored on the same disk location. If a user transfers a file to the 'Trash' and then empties it securely, this specific file has been securely erased. However, any copies of the file made before that time have therefore not been securely erased and can still be 'recovered'. In order to not provide users with a false feeling of security, Apple has removed both options with the introduction of the newest version of its operating system, El Capitan (Mac OS X 10.11).¹⁶

Even more important is a second observation relating to the operation of the email program 'Mail' on an Apple computer. In order to prevent loss of data or disruption of the proper operation of programmes, various folders with files are by default not accessible for users.

On an Apple computer, - as opposed to, for example, Microsoft Exchange and Microsoft Outlook¹⁷ - an individual email message is an individual file with an .emlx file extension. These files are stored in a file location with, for example, the following path for sent messages:¹⁸

/Users/username/Library/Mail/V2/POP-useraccount/Sent messages.mbox/@@@/0/1/1/Data/Messages/

In the more recent versions of Mac OS X, the Library folder is no longer shown. The user can only view this folder by holding a special key while clicking the parent folder.

¹⁶ The possibility still exists within the operating system, but is no longer offered in the graphical user interface. In order to still apply the functionality, the user must open a session in the program Terminal after which a Unix command can be executed. For example, in order to completely overwrite the free disk space 7 times, the command is 'diskutil secureErase freespace 2 /Volumes/drivename'.

¹⁷ Microsoft Exchange is the mail server application of Microsoft which is responsible for the email traffic within a network. This application stores all email messages of all users of the mail server in a central database (these files have an .edb extension). Microsoft Outlook is a mail client. A user can, among other things, subsequently make a connection with his/her 'mailbox' on the mail server. For offline use, the user can synchronise his/her 'mailbox'. The mail messages are then copied to one locally stored file (with an .ost extension). A user can also choose to archive email messages locally. This also takes place in one locally stored file (with a .pst extension).

¹⁸ Here, @@@ stands for a randomly comprised folder name, consisting of hexadecimal characters,



The operating system also shows to contain files with an .mbox extension. These are in fact also folders, the contents of which only become visible by holding a special key while clicking the folder. If the user nevertheless manages to gain access to the lowest level, where the individual messages are shown as .emlx files, then it is still not easy to find the file that the user wishes to delete: the files have numbers as file names. The messages must be opened in order to see the specific message. Once the message has been found, it can be subsequently moved to the 'Trash' in order to securely erase it in the above described method. In order to securely erase individual email messages, specialized knowledge of the Mac OS X operating system is required which a regular user does not have.¹⁹ Furthermore, there exists the risk that the individual deletion - outside of the Mail program - disrupts the operation of the mail program as a result of which the mail boxes must be rebuilt.

An alternative approach is that messages are first deleted in the Mail program and that subsequently, with the help of a tool, the free disk space is completely overwritten with meaningless information. However, we have found no indications for the use of such tools in the above.

5.5 Evaluation

The pictures found after data carving - which visually resemble one or more of the 1,250 Pictures (in original size) - concern embedded pictures reduced in size, without EXIF data, which were stored on the Client's hard disks by receipt per email of four PDF files, contained in Exhibit L.

As indicated above, we have found none of the 1,250 Pictures (in original size) among the images stored on the hard disks of the Client's computers.

We deem it most unlikely that one or more of the 1,250 Pictures (in original size) have been stored on the hard disks of the Client's computers but have been deleted in a secure, irrecoverable manner. After all, no indicators were found for the complete overwriting of the free disk space. The secure erasure of individual email messages and related attachments requires highly specific IT knowledge, and what's more, with the most recent versions of Mac OS X (as in any case used on the 'MacBook Primary') the secure erasure of files offers no certainty that all existing copies of the specific files are erased.

Since none of the original 1,250 Pictures were stored on the hard disks of the Client's computers, we deem it most unlikely that the files were sent per email from the Client's computers to the counterparty, or at least to Buiter. All the more because the secure and irrecoverable erasure of specific email messages requires many actions and very specific IT knowledge and furthermore no indicators were found for the overwriting of free disk space.

6 Email messages 'me myself and I'

As already indicated in paragraph 3.3, the Client's Dutch lawyer informed us that the Client sent several email messages to Buiter in mid 2011. The subject of these messages was always 'me myself and I'. These messages included an attachment with a

¹⁹ As an alternative method, a user can open a session in the program Terminal. Then the user can navigate through the folder structure directly, by using Unix commands. The folder structure is directly visible then. The use of the Terminal possibly requires even more extensive IT knowledge.



file named 'moi.jpg.' This relates to a picture that the Client acknowledges to have created herself.

After inspection of the 'moi.jpg' file it appeared to include various EXIF-data. It concerns among other things the recording date ('7-6-2011'), the camera manufacturer ('Research in Motion', the manufacturer of Blackberry smartphones), the camera model ('Blackberry 9300'), the flash mode ('No flash'), and the picture resolution ('72 dpi'). The picture size is 804 x 1,072 pixels.

We have found no file titled 'moi.jpg' on the images of the hard disks of the Client's computers, nor did we find any email messages with the subject 'me, myself and I'.

In combination with the EXIF data presented above, we therefore deem it most unlikely that the specific photo was made with a Blackberry smartphone. It is, however, possible that this picture was sent using a Blackberry smartphone.

Perhaps superfluously, we would like to remark that we deem it most unlikely, based on the file properties described above in chapter 4 of this report, that the 1,250 Pictures were captured with a Blackberry smartphone.

7 Email messages 'I miss you'

On 31 July, 3 and 4 August 2010, Client sent a total of four email messages to Buiter with either 'I miss you' or the Dutch '*Ik mis je*' as subject. A picture, by the title 'plaatje.jpg', was attached to these messages.

We found the original picture on the image of the 'MacBook Pro', in the 'Photo Booth' folder. This folder is used by the Photo Booth-application as default storage location and is created upon the first use of this application in the user's 'Pictures' folder.

In the EXIF data of this picture, we only found the picture size (640 x 480 pixels). Insofar as we have been able to verify, the Photo Booth application has no options to set the picture size of the images. We furthermore established that the picture resolution is not stored in the EXIF data. As IPTC label is stated the name of the application with which the picture is created ('Photo Booth').

Perhaps superfluously, we would like to point out that it is most unlikely that the Pictures, just like the picture attached to the above-discussed email messages, were created with the use of Photo Booth, for the reason that among the Pictures there are also photos with a deviating, smaller picture size than the default picture size of Photo Booth, but also because the picture resolution of the version of Photo Booth used by Client, or at least the version on the 'MacBook Pro' does not store the picture resolution in the EXIF data, and finally considering the absence of the other EXIF data, such as the flash mode, and the presence of the IPTC label 'Photo Booth'.

8 Rule for storing attachments

8.1 Introduction

The Client's Dutch lawyer has informed us that Buiter declared in an Affidavit dated 11 August 2015 that he installed a small program which ensured that attachments to



email messages were saved separately to a specifically designated location. An example of such a program was allegedly attached to the Affidavit as Exhibit 9.

The Client's Dutch lawyer has provided us with a copy of the Affidavit and Exhibit 9, in order to assess the use of this 'program'.

8.2 The way the 'rule' works

Exhibit 9 contains a print of a message on an internetblog, 'Pixelchef.net'. From this it can be deduced that the terminology used by Buiter in the Affidavit is incorrect, or at least inaccurate: there is no 'program' that can be 'installed'.

Email programmes such as Microsoft Outlook, as apparently used by Buiter, usually have the option to automate simple, common tasks. This is done in Outlook by setting a so-called 'rule'. With the help of such a rule a user can, for example, relocate all messages received from a specific email address to a specific folder.

Visual Basic for Applications (VBA) is a feature developed by Microsoft with which 'scripts' (a set of instructions) can be written which can change or expand the functionality and/or operation of applications that support VBA, such as Microsoft Outlook.

In Exhibit 9 is explained how a user can set a 'rule' in Outlook, which runs a VBA script upon receipt of an email message. The VBA script shown in Exhibit 9 stores the attachment to an email message in a folder designated for that purpose in the script.

The original email with the attachment is not replaced or removed as a consequence of the 'rule'. Use of this 'rule' and the application of the script ran by that rule, does also not lead to any changes in the file name.

If several attachments are received with the same file name, the script will overwrite the older file with the same name. For users who do not wish this, the writer of the blog offers the following option as a solution: change some lines in the script to store the attachments with the storage date and time added to the file name.

One cannot deduct from the Affidavit whether Buiter chose this option or went with the standard script.

The counterparty argues that the Pictures were sent by Client to Buiter per email. If this were the case, it is theoretically possible that some photos were sent several times by Client per email. Based on general user habits on the one hand and the fact that the email messages discussed in chapters 6 and 7 were sent several times and were each time accompanied by an attachment with the same file name, we deem it most unlikely that Client used different file names each time she sent one of the Pictures.

This implies that the same file must have been stored several times by the 'rule', in the location as indicated by Buiter in the script ran by that 'rule'. If the standard script of Exhibit 9 had been used there would have been no double Pictures, since this would have resulted in the overwriting of earlier files with the same file name. In that case Buiter must have used a modified script. If he would have chosen for the solution mentioned in Exhibit 9, the file names of the Pictures should include the storage date and time. However, this is not the case for the 1,250 Pictures on the USB stick.



In this context it is furthermore important to remark that the images discussed in chapters 6 and 7 were sent by email to Buiter several times. Therefore, if the 'rule' was used, these images should be stored on Buiter's hard disk.

The picture in the 'moi.jpg' file is not part of the Pictures on the USB stick, and an image that bears a strong resemblance to the image in the 'moi.jpg' file only appears once in the PDF files of Exhibit L. The image in the 'plaatje.jpg' file is not part of the Pictures on the USB stick and there are no images among the PDF files of Exhibit L that show a strong visual resemblance to the image in the 'plaatje.jpg' file. These findings are not in accordance with the way the 'rule' works.

8.3 Ratio for the use of the 'rule'

In paragraph 11 of the Affidavit, Buiter states that he regularly receives email messages with large attachments which he subsequently has to store. He says that he used the 'rule', or something similar, in order to prevent that, briefly put, the - at the outset - limited storage capacity of the Outlook mailbox would be exceeded as a result of keeping these attachments in Outlook.²⁰

As a solution for this problem, the option for a 'rule' as described in Exhibit 9 is remarkable, in the sense that the original email with the attachment is not removed from the Outlook mailbox by means of the 'rule'. The risk of exceeding the storage capacity thus remains, unless the user decides to manually remove these email messages from the mailbox. That is why the 'rule' only results in a very limited time advantage but with a serious disadvantage: what remains is a folder with files in respect of which it is no longer possible to establish how these were received, who sent them and which remarks accompanied these files.

There are easier and more effective solutions for the problem signalled by Buiter: a user can set a 'rule' in Outlook with which every email message containing an attachment is moved to a local archive (a locally stored file with a .pst extension). The advantages of this procedure are that the size of the mailbox is reduced directly, the context of the attachment is retained, and that one can still use the search options of Outlook. Such a 'rule' is furthermore much easier to realize, because it can be set with the support of a 'Wizard' in Outlook and no complicated VBA script has to be written and addressed.

8.4 Evaluation

The rule described in Exhibit 9 is an unnecessarily complicated and not very effective solution for the problem identified by Buiter of the (initially) limited mail box capacity in Outlook.

The fact that on the one hand certain of the Pictures are stored twice and on the other hand various versions of "moi.jpg" are missing and the image "plaatje.jpg" is missing altogether, is not consistent with the way the specific "rule" works.

²⁰ Up to and including Outlook 2002, the maximum size of the file in which all mail items, contacts, etc. are stored (the Outlook.pst file) is almost 2 GB. The standard limit for Outlook 2003 and 2007 is 20 GB, and for newer versions the limit is 50 GB. Incidentally, these standard limits can be increased for the versions Outlook 2003 and onwards. What's more, storage capacity can easily be increased by creating locally stored archive files.



9 Concluding remarks

We received 1,250 files on a USB stick. The file names of the Pictures run from (1).jpg up to and including (1387).jpg. Various intervening numbers are missing.

Given the customary naming conventions, we consider it more than likely that, after the initial storage of the Pictures, the file names were modified afterwards.

Given the Client's position in the pictures, she was not able to operate the recording device. Based on the compositions and content of the pictures it is most likely that the photographs belonging to the same series were made one shortly after the other. This indicates that no 'self-timer' was used. It is most likely that the Pictures are not the result of acts carried out by the Client.

The picture size, the aspect ratio and content of the Pictures are consistent with the use of a webcam or a mobile telephone. However, the files contain little EXIF data. That is a strong indicator that the Pictures were not recorded using a digital camera or mobile telephone.

It is most unlikely that the Pictures are the result of saving separate images from a video file.

It is most likely that the Pictures were created using a webcam in a Windows environment. This is indicated by the fact that the Pictures according to the EXIF data have an image resolution of 96 dpi. It is most unlikely that the Pictures were stored on an Apple computer as used by the Client.

It cannot be excluded that the form, size and resolution of the file or the file format have been modified after the original creation. However, in that case the Pictures would have to have been stored on the Client's hard disks at a certain moment. No indicators were found for that.

Based on the hash values of all Pictures on the images, it can be concluded that none of the 1,250 Pictures were found on the images of the Client's computers. The images were also examined for deleted files. Based on the hash values it can be concluded that none of the 1,250 Pictures have been stored on the Client's computer, but were later deleted and could still be fully recovered.

On the "Macbook Pro" and the "Macbook Primary" various pictures were found that show a strong visual resemblance to one or more of the 1,250 Pictures. This concerned removed copies of the files "Exhibit L Photographs Mees Sent Buiter [number].pdf". The pictures contained therein could not be found based on the hash values, because these pictures were recorded without EXIF data and in a smaller format in the PDF files.

Given the fact that the computers most likely were used intensively and given the large number of files that could be recovered, it is most likely that no tool was applied to the computers to overwrite free disk space.

The picture "moi.jpg" was most likely made using a Blackberry smartphone. This opinion is based on the EXIF data of the picture, which contain the camera manufacturer and the camera model. It is possible that this picture was also sent using a Blackberry smartphone. E-mail messages with this picture as an attachment were in any case not found on the Client's computers.



The picture "plaatje.jpg" which the Client sent to Buiter several times by email was most likely created using the application Photo Booth on the "Macbook Pro".

Given the differences in file properties, it is most unlikely that the 1,250 Pictures were recorded the same way as the picture "moi.jpg" or the picture "plaatje.jpg".

In summary, the observations and conclusions set out above lead to the following final conclusion:

- It is most unlikely that the 1,250 Pictures were recorded by the Client herself. Due to the quick succession of the photographs it is most unlikely that a self-timer was used.
- It is most unlikely that one or more of the 1,250 Pictures (in original size) were once stored on the hard disks of the Client's computers and then deleted in a secure, irrecoverable manner.
- No indicators were found for the complete overwriting of the free disk space. The secure removal of individual email messages and related attachments requires highly specific IT knowledge.
- It is most unlikely that the Pictures were sent by email to the opposing party or at least to Buiter using one of the Client's examined computers.

We trust to have been of sufficient service to you by issuing this report.

SBV Forensics B.V.

On whose behalf

A handwritten signature in black ink, appearing to read "M.G.J. de Gunst", written over a horizontal line.

M.G.J. de Gunst MSc LLM